DATA RECON

User Guide

GROUND LABS

Data Recon

Table of Contents

DATA RECON 2.0.25 RELEASE NOTES

New Data Types

- New data type: Belgium national ID.
- New data type: Bulgaria national ID (EGN).
- New data type: Cyprus passport number.
- New data type: Denmark driver's license.
- New data type: Denmark passport number.
- New data type: Hungary Personal Identification Number (PIN).
- New data type: Ireland passport card.
- New data type: Ireland passport number.
- New data type: Korean bank account numbers (NongHyup Bank, KB Bank, KEB Hana Bank).
- New data type: Malta national e-ID.
- New data type: Slovakia and Czech Republic national ID (updated).
- New data type: Slovenia national ID (EMŠO).
- New data type: Sweden driver's license.
- New data type: Sweden identity card.
- New data type: Sweden passport number.
- 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.
- Improved: Support for South Korean driver's license.
- 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.fodt files.
- False positives: Removed false positives that occur with the Turkish PIN.

ABOUT DATA RECON

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

OVERVIEW

DATA 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), **DATA 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, **DATA RECON** is the PCI compliance tool of choice for more than 300 Qualified Security Accessors (QSAs), and trusted by over 2,500 merchants across 80 countries. Support for more than 7+ operating systems and the ability to scan cloud storage means that **DATA RECON** can cover the majority of common system types used by organizations.

Who is DATA RECON Suitable For

DATA RECON is ideal for security consultants and small businesses with a requirement to scan up to 5 systems. **DATA RECON** Standard Edition is designed for scanning the contents of Workstations whilst **DATA 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

1. Advanced support: https://www.groundlabs.com/submit-a-ticket/
2. Ground Labs home page: https://www.groundlabs.com
3. **DATA RECON** End User License Agreement: https://www.groundlabs.com/eula/

FEATURES

- **Built for PCI Compliance**: Out-of-the-box cardholder data detection for 10 major card brands that can find 160+ combinations of PAN structures used across more than 200 countries.
- **Accurate and Powerful**: Our data discovery algorithms are extensively tested to produce fast and accurate search results; false positives are managed by a built-in detection algorithm that filters test results to keep your scans effective.
- **Search almost Anything**: This software searches a wide range of offline and online storage locations, including workstations, file servers, NAS and SAN devices, Gmail, IBM Notes and Oracle.
- **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**: **DATA 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 **DATA RECON**. Use of **DATA 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.

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

SYSTEM REQUIREMENTS

DATA 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 **DATA 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.

Category	Operating Systems
Windows Desktop Environments (GUI and Command-Line)	• Windows XP • Windows XP Embedded • Windows Vista • Windows 7 • Windows 8 • Windows 8.1 • Windows 10
Windows Server Environments (GUI and Command-Line)	• Windows Server 2003 R2 • Windows Server 2008/2008 R2 • Windows Vista • Windows Server 2012 • Windows Server 2016
Linux System Environments (Command-Line only)	• CentOS • Debian • Fedora • Red Hat • Slackware • SUSE • Ubuntu A minimum Linux Kernal version of 2.4 is required.

Category	Operating Systems
UNIX System Environment (Command-Line only)	• Solaris 9.x – 11.x (SPARC & Intel x86) • AIX 6.1 – 7.1 • FreeBSD 9+ (Intel x86) • HP UX 11.31+ (Intel Itanium) • Macintosh – OSX 10.5+ (Intel x86 & PowerPC)
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).

GETTING STARTED

DATA RECON requires no installation to run scans.

SYSTEM REQUIREMENTS

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

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

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

DOWNLOAD DATA RECON

If you have not obtained a licensed copy of **DATA RECON** you can get a free trial, or purchase **DATA 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 **DATA RECON** version that matches your operating system
    - **DATA RECON** Command-Line Interface (CLI) applications.
    - **DATA 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 DATA RECON

Note: Administrator privileges are required for **DATA RECON** to run. This guide assumes that you are running **DATA RECON** on the host you wish to scan and that you are scanning the host's local storage.

Once downloaded, locate the **DATA RECON** executable in your downloads folder. By default, **DATA 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 `datarecon` and move your **DATA RECON** executable into it.

WINDOWS GUI

To set up **DATA RECON** with the Windows GUI:

1. Create a new folder in Windows Explorer
2. Move the **DATA RECON** executable to the new folder

LINUX SHELL

In your terminal, run the following commands:

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

# Moves the DATA RECON executable to the ~/datarecon/ directory
mv datarecon_linux26_2.0.xx datarecon

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

RUNNING DATA RECON AS A PORTABLE APPLICATION

DATA RECON is a portable application.

You can put **DATA RECON** on a portable storage drive and run it on any authorized host system.

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

To run DATA RECON as a portable application:

1. Download the appropriate version of **DATA RECON** for your system.
2. Download an OFFLINE LICENSE FILE. See Offline Authentication.

3. Place the OFFLINE LICENSE FILE in the same folder as your **DATA RECON** executable.
4. Run **DATA RECON**.

RUNNING THE DATA RECON GUI

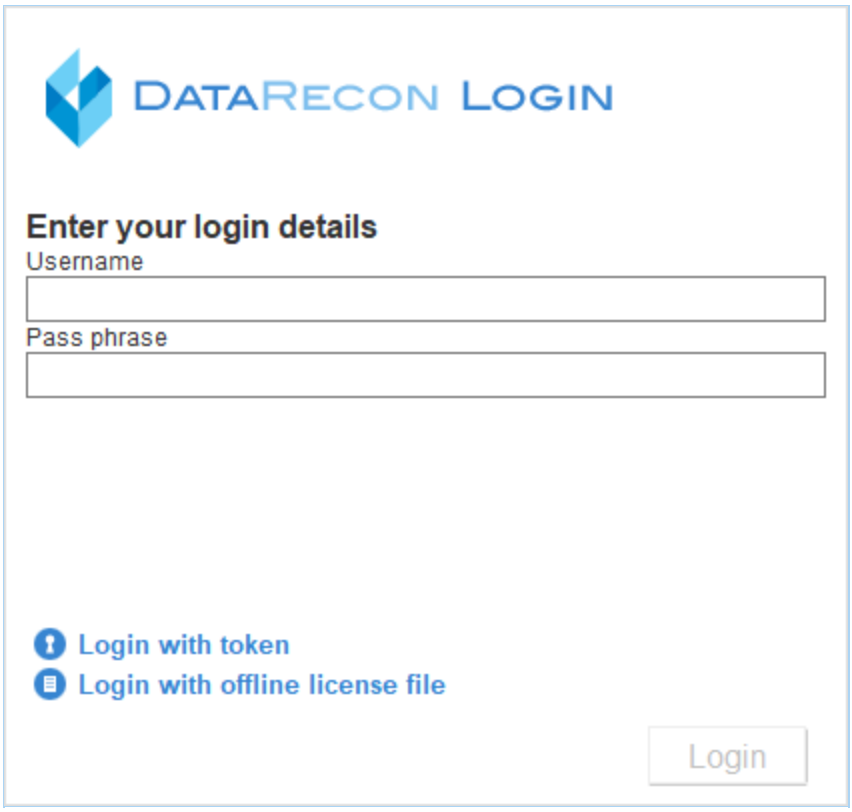
Info:
When the **DATA RECON** runs, it looks for these files in its directory:

- `datarecon.cfg` : default **DATA RECON** configuration file.
- `<license-file-name>.li2` : OFFLINE LICENSE FILE; **DATA RECON** looks for any file ending with `.li2` .

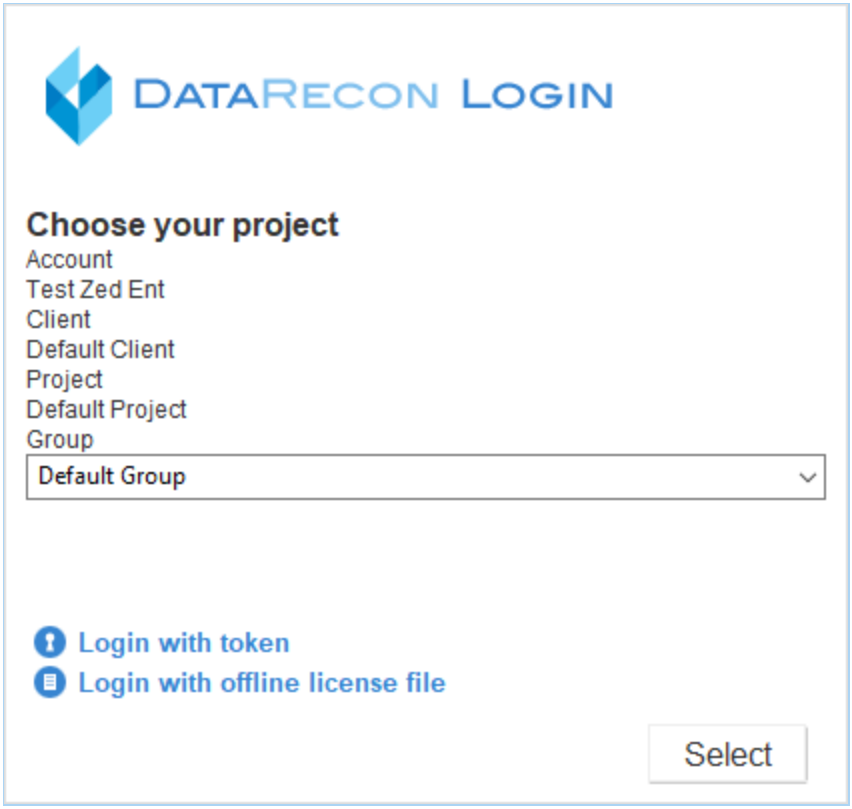
If it finds any of these files in the directory that the **DATA RECON** executable occupies, it will try to load them when the **DATA RECON** runs.

To run **DATA RECON**:

1. Double-click on the **DATA RECON** executable (e.g. `datarecon_gui_2.0.xx.exe`) to run **DATA RECON**.
2. In the **DATA RECON** login window, enter your Ground Labs Services Portal user name and password.

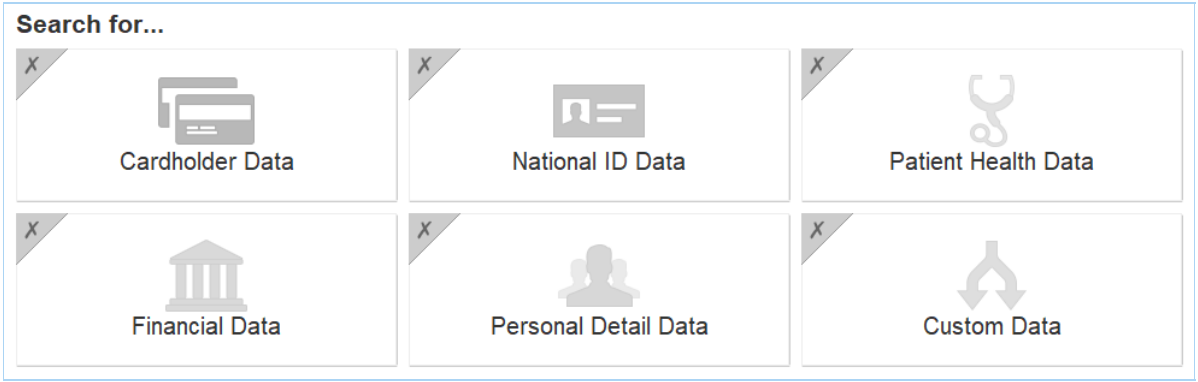


3. From the **Choose your project list**, select your project and click **Select**.

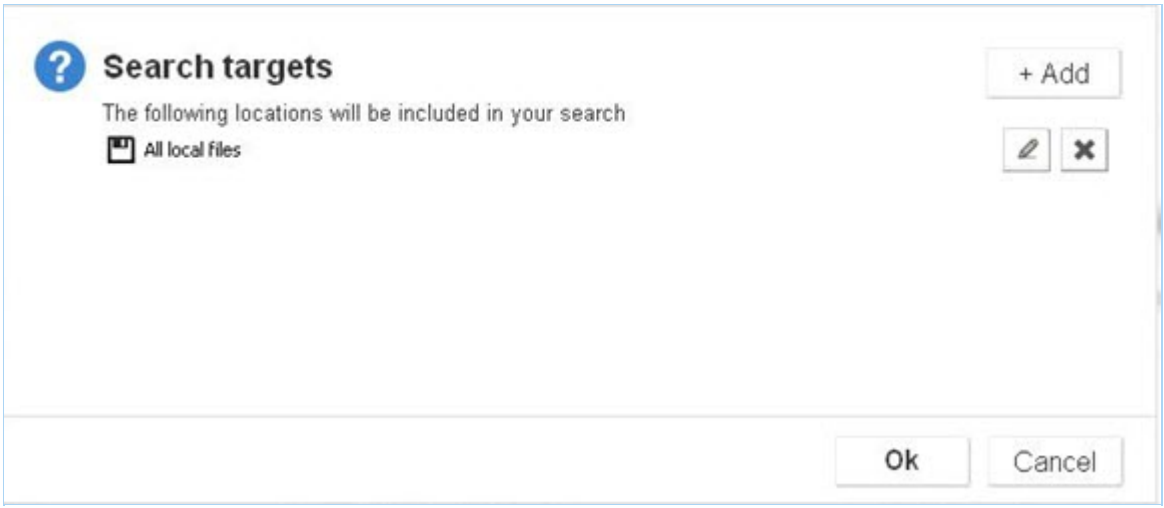


> **Note: Managing licenses**
> Project and license groups are usually used by the licensees or IT administrators who manage your software licenses to assign permissions to certain groups of users.
>
> If you are not sure of which project or license group to use, contact your IT administrator or the 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 DATA RECON Licensing.

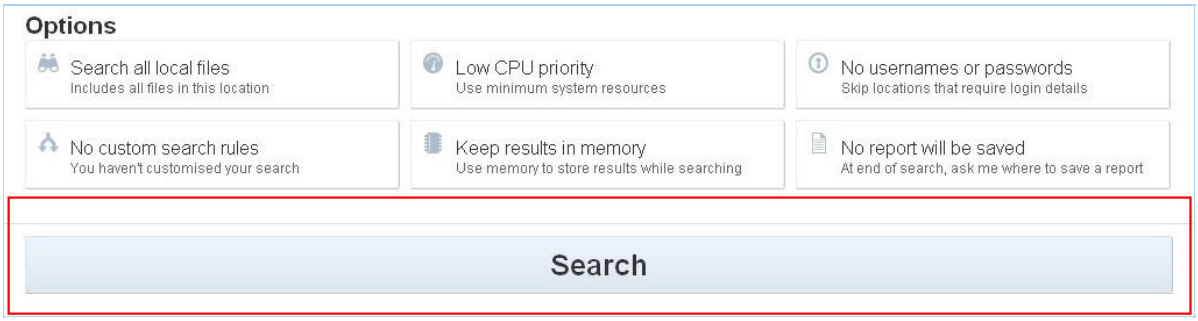
4. On the dashboard, select the card data types to include in your scan.



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



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



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

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

RUNNING THE DATA RECON CLI

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

> **Info:**
> When the **DATA RECON** runs, it looks for these files in its directory:
>
> - `datarecon.cfg` : default **DATA RECON** configuration file.
> - `<license-file-name>.li2` : OFFLINE LICENSE FILE; **DATA RECON** looks for any file ending with `.li2` .
>
> If it finds any of these files in the directory that the **DATA RECON** executable occupies, it will try to load them when the **DATA RECON** runs.

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

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

For more information, see DATA RECON CLI Options.

RUNNING THE DATA RECON CLI ON WINDOWS

Locate the Windows CLI executable: `datarecon_2.0.xx.exe`

There are 2 ways to run the Windows CLI.

Method 1

1. Locate `datarecon_2.0.xx.exe` in Windows Explorer.
2. Right-click `datarecon_2.0.xx.exe` , select **Run as administrator** and enter the administrator password if prompted.
3. In the terminal, **DATA RECON** will prompt you to validate your license
4. Log in using one of the three methods (see Logging into DATA RECON for more information):
    - Ground Labs Login.
    - Use an online token.
    - Use offline license file.

> **Info:** **DATA 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.

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 **DATA RECON** executable is located.

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

5. To run the **DATA RECON** executable with default settings, issue this command:

```
# Run a default scan, save a compliance report and an encrypted database journal file.
datarecon_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 **DATA RECON** GUI.

6. **DATA RECON** prompts you to validate your license.
7. Log in using one of the three methods (see Logging into DATA RECON for more information):
   - Ground Labs Login.
   - Use an online token.
   - Use offline license file.

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

8. Once logged in, **DATA RECON** runs a scan with default settings. When the scan completes, **DATA RECON** automatically saves a compliance report.

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

RUNNING THE DATA RECON CLI ON LINUX AND UNIX-LIKE SYSTEMS

1. In the Terminal, locate the **DATA RECON** executable. E.g. `datarecon_linux26_2.0.xx` .
2. Open your terminal and run:

```
chmod u+x datarecon_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.
./datarecon_linux26_64_2.0.xx -j journal-filename.jnl -password-inline password
```

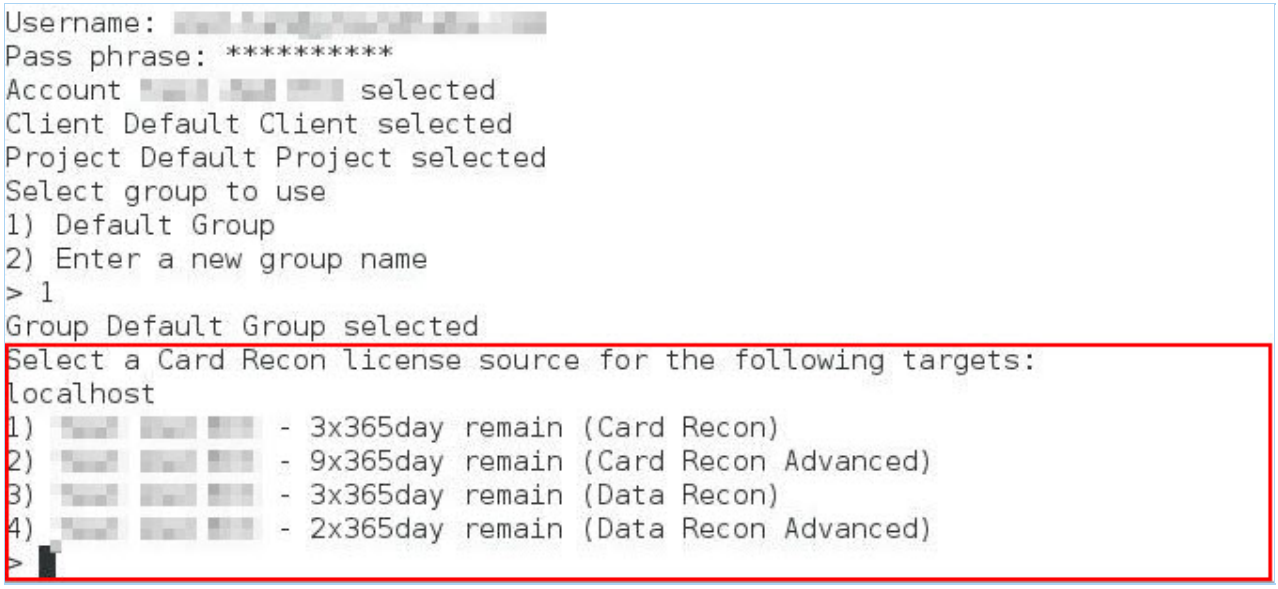
4. **DATA RECON** prompts you to validate your license.

> **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 DATA RECON Licensing.

5. Log in using one of the three methods (see Logging into DATA RECON for more information):
   - Ground Labs Login.
   - Use an online token.
   - Use offline license file.

> **Info: DATA 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, **DATA RECON** will return a list of licenses available in your Ground Labs Services Portal.



DATA RECON should ask you to confirm authorisation of the TARGET. For more information on **DATA RECON** licensing, see DATA RECON Licensing.

DATA RECON starts scanning the TARGET with default settings.

Once done, **DATA RECON** automatically saves a compliance report. To inspect and remediate matches found by **DATA RECON**, load the database journal file (e.g. `journal -filename.jnl`) saved by the **DATA RECON** CLI in the **DATA RECON** GUI (see Results and Remediation).

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

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

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

DATA RECON LICENSING

This section covers the following topics:

SUBSCRIPTION LICENSE

DATA 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	**All servers**: 1 license per server. This allows you to run scans on the local file system, process memory, and on network storage. **Info:** 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.
	Database servers: 1 license per database server. Database servers are licensed individually. If using a clustered database, each node must also be individually licensed.
	Websites: 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: • example.com • www.example.com • subdomain.example.com
Google Apps/ G Suite	1 license per user across Google Mail, Google Calendars, Google Tasks, and Google Drive storage.
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.

Target Type	License Assignment
Google Mail (Gmail)	See Google Apps/ G Suite for more information. Must have IMAP enabled.
IBM / Lotus Notes	1 license per IBM / Lotus Notes user.
IMAP/IMAPS Mailboxes	1 license per internet mailbox (IMAP/IMAPS).

DATA RECON STANDARD EDITION AND ADVANCED EDITION

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

To use **DATA RECON** to scan advanced TARGETS such as databases and cloud storage, you would need to upgrade to a **DATA 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		✓
Note: Some features are not available on all supported operating systems.		
File Formats		
Text Files	✓	✓
Multiple Encoding types	✓	✓
Office Documents	✓	✓
Compressed Files	✓	✓
Databases (client side)	✓	✓
Databases (server side)		✓
Emails (client)	✓	✓

Platform or File Type	Standard Edition	Advanced Edition
Emails (server)		✓
Audio Files		✓
Image File OCR		✓
Target Types		
Local Storage	✓	✓
Free Disk Space	✓	✓
Shadow Volumes	✓	✓
Process Memory	✓	✓
Websites	✓	✓
Network Storage		✓
Live Database Servers		✓
Live Email Servers		✓
Cloud Storage		✓
Database Servers (Live)		
IBM DB2		✓
Microsoft SQL Server		✓
MySQL		✓
Oracle		✓
PostgreSQL		✓
SAP Sybase		✓
Email Servers		
Gmail (IMAP)*		✓
Generic IMAP*		✓
IBM / Lotus Notes*		✓
Cloud Storage		
Google Apps		✓
Microsoft Azure		✓
Rackspace		✓
Classification and Remediation		
Mask Cardholder Data	✓	✓
Secure Quarantine	✓	✓
Permanent Delete	✓	✓

Platform or File Type	Standard Edition	Advanced Edition
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 Ground Labs EULA for more information.

Before a scan can be run on a TARGET with **DATA 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.

Note: By default, **DATA RECON** will assume that the local storage system of host (the computer that **DATA 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 DATA RECON.

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.

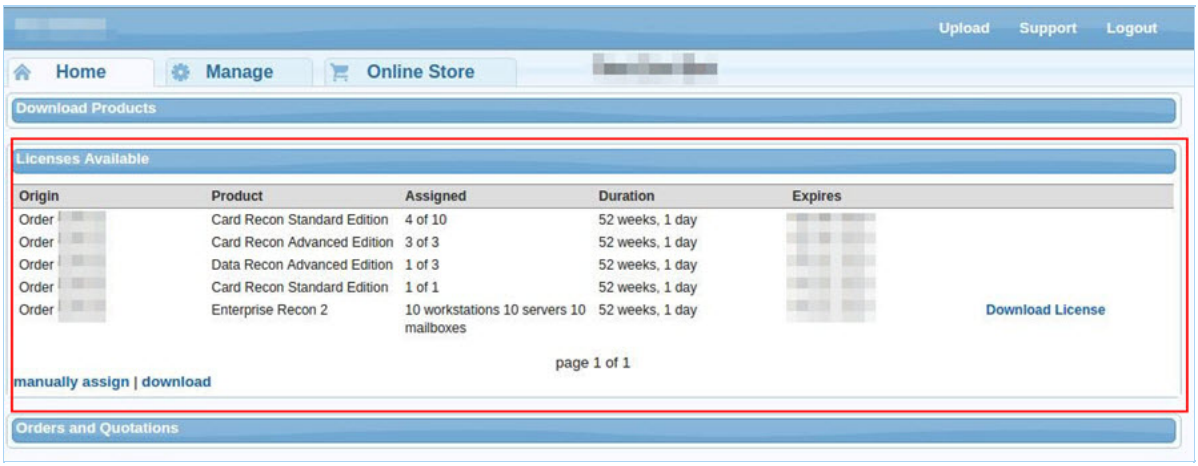
See Online Authentication for more information.

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

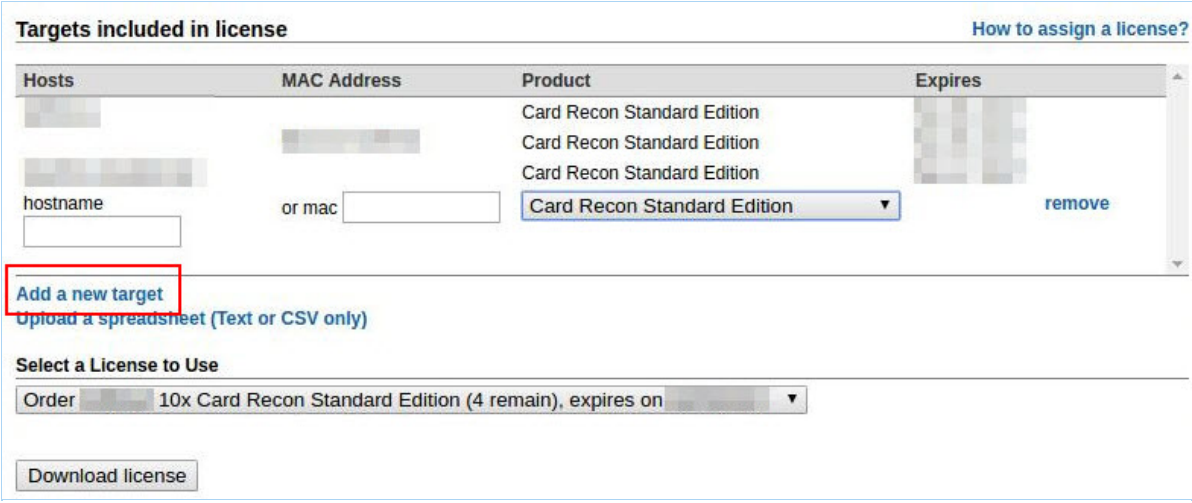
ASSIGNING A LICENSE THROUGH THE GROUND LABS SERVICES PORTAL

To assign a license to a TARGET:

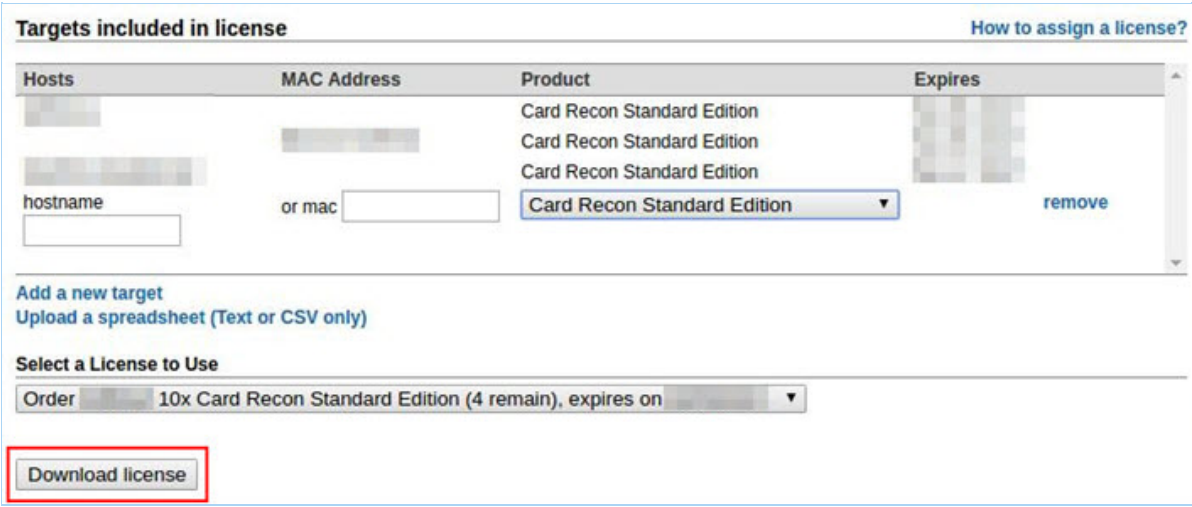
1. On to the Ground Labs Services Portal, go to the **Licenses Available** section to see a summary of the licenses that are associated with your account.



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



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



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

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

OFFLINE LICENSES

Downloading a license will put an OFFLINE LICENSE FILE (`*.li2`) in your downloads folder. This license file can be used to authenticate your copy of **DATA RECON** without an Internet connection.

For more information on using offline licenses, please see Logging into DATA RECON.

ASSIGNING LICENSES THROUGH OTHER MEANS

You can also assign licenses through the **DATA RECON** application itself.

To assign a license through the **DATA RECON** application, you will either need a Ground Labs Services Portal account or a SCAN TOKEN. For details, see Generating and Using Scan Tokens.

Log into the **DATA RECON** application using your Ground Labs Services Portal account or SCAN TOKEN.

When you attempt to scan an unlicensed TARGET, **DATA RECON** will prompt you to assign an available license to that TARGET.

For more information on assigning licenses through other means, see Logging into DATA RECON.

Info: When attempting to scan an unlicensed TARGET while logged in with a SCAN TOKEN, **DATA 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 **DATA RECON** will return an “Insufficient available licenses” error and not allow you to assign additional licenses.

GETTING HOST NAME AND MAC ADDRESS

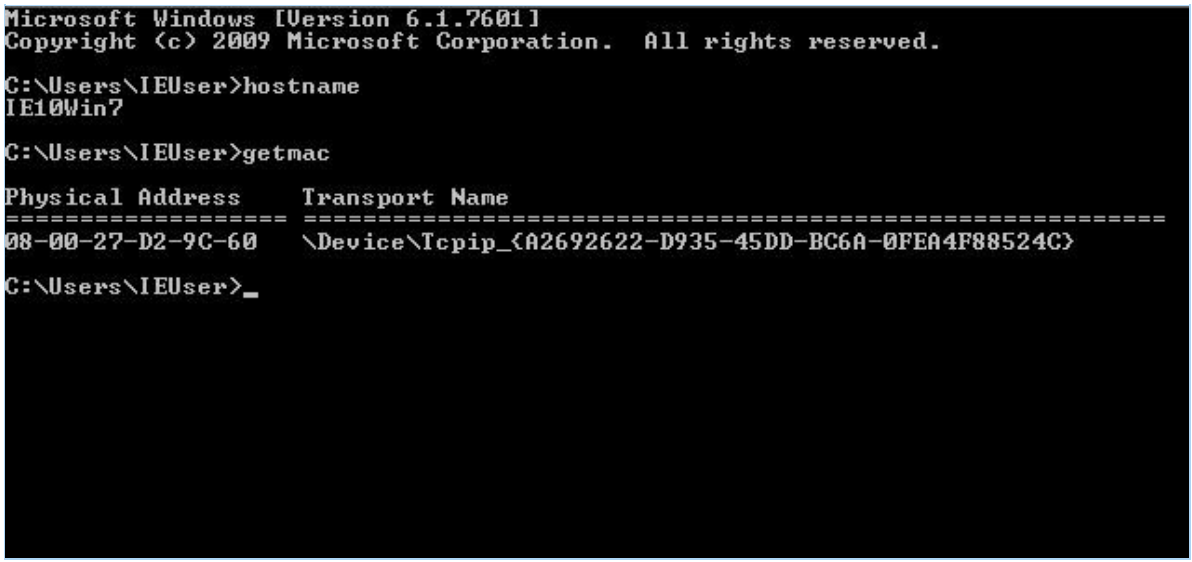
You will need either the `hostname` or the MAC address of the TARGET to assign it a license through the Ground Labs Services Portal.

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

WINDOWS SYSTEMS

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

```
hostname
getmac
```



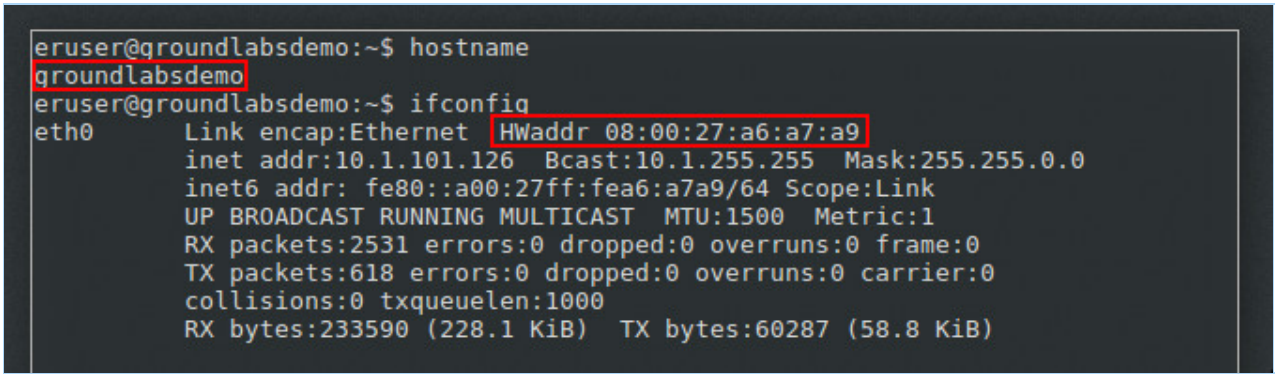
   - `hostname` gets the command prompt to return your Windows machine's host name.
   - `getmac` gets the command prompt to return your machine's MAC address (also known as the machine's physical address).

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

Open the terminal and issue the following commands:

```
hostname
ifconfig -a
```

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



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

LOGGING INTO DATA RECON

You need to log into **DATA RECON** before you can use the application. You can log into **DATA RECON** through:

- Online authentication.
- Offline authentication.

Note: Online authentication requires a working Internet connection. This means that the host running **DATA 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 **DATA RECON** to authenticate online.

ONLINE AUTHENTICATION

Online authentication requires a working Internet connection. This means that the host running **DATA 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 **DATA RECON** to authenticate online.

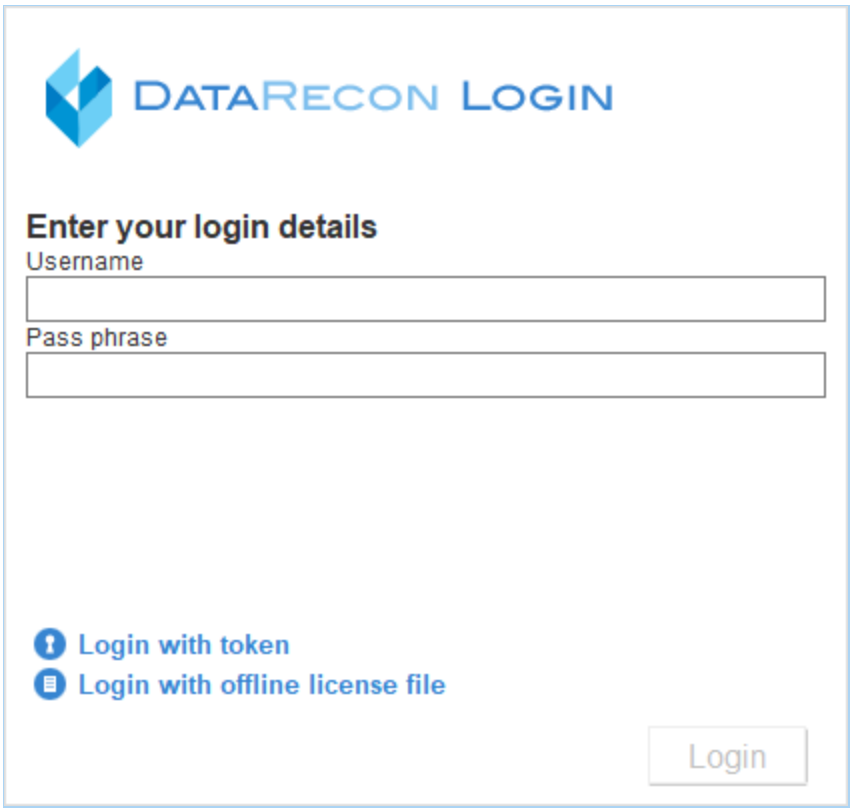
DATA RECON will attempt to connect to Ground Labs's authentication servers; if it cannot connect to the authentication servers, **DATA RECON** will return a "Can't connect to licensing system" error and will not allow you to continue using **DATA RECON**.

You can authenticate online using:

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

Ground Labs Services Login

You can log into DATA RECON using your Ground Labs Services Portal username and password.



DATA RECON will connect to the Ground Labs authentication servers and verify your login details.

If you log in using your Ground Labs Services Portal account, **DATA 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, **DATA 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 **DATA RECON** with a SCAN TOKEN.

Using a SCAN TOKEN to log into **DATA RECON** would mean that **DATA RECON** would use licensing information associated with the SCAN TOKEN.

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

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

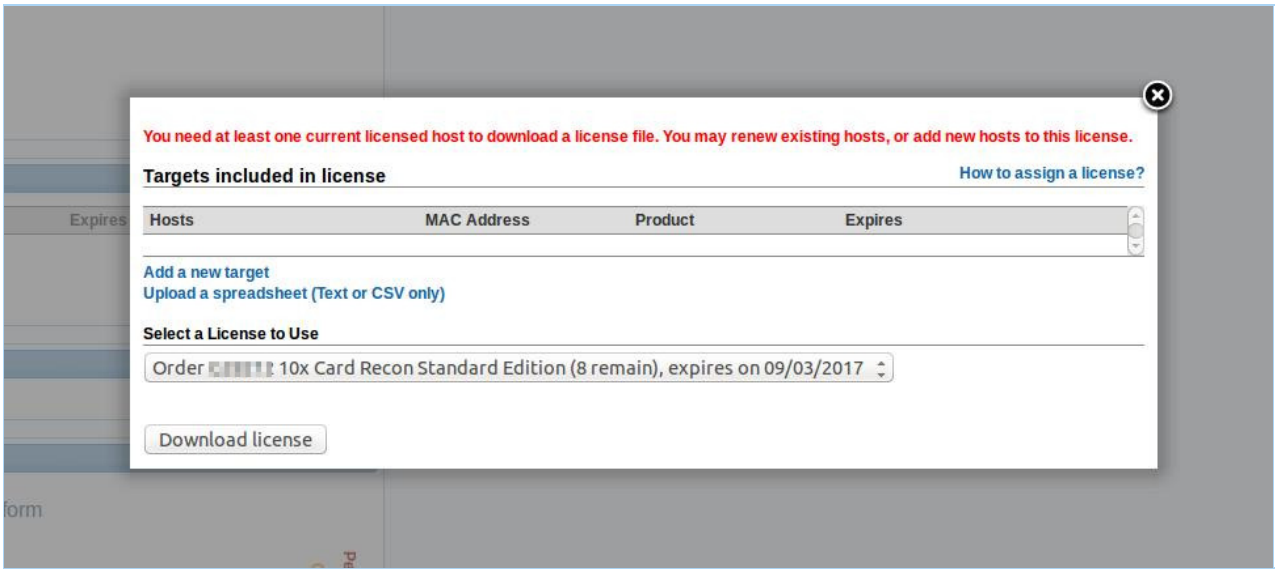
If the TARGET has a license already assigned to it, using a SCAN TOKEN will not use an additional license if the existing license and the SCAN TOKEN are from the same Ground Labs Services Portal parent account.

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

OFFLINE AUTHENTICATION

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

The Ground Labs Services Portal allows authorized users to download OFFLINE LICENSE FILES (`*.li2`).



You must assign at least one license to a TARGET before you can download an OFFLINE LICENSE FILE.

Once you have assigned a license to a TARGET, you'll be able to download an OFFLINE LICENSE FILE. If no TARGET has been assigned, the Ground Labs Services Portal will return an error.

Look for the "Licenses Available" section on the Ground Labs Services Portal dashboard. Click download to download the OFFLINE LICENSE FILE.

There are 2 ways to use OFFLINE LICENSE FILES in the **DATA RECON** CLI and GUI:

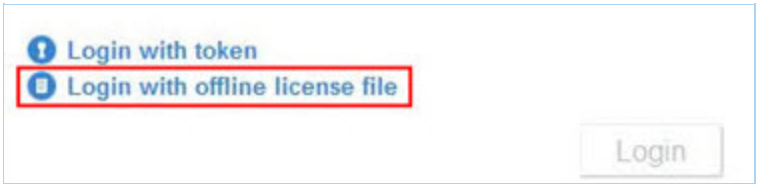
- Selecting the **Login with offline license file** option at the **DATA RECON** login screen.
- Placing the OFFLINE LICENSE FILE in the same folder as the **DATA RECON** executable.

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

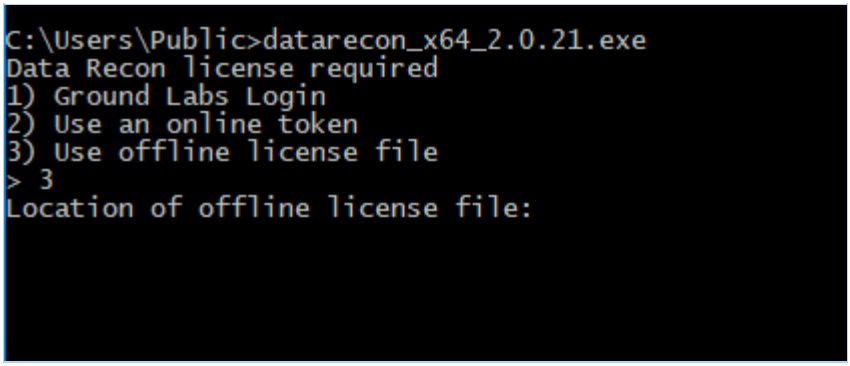
On the Windows GUI, the **Login with offline license file** option can be found on the login screen.



Selecting that will get **DATA RECON** to prompt you to locate your OFFLINE LICENSE FILE on your disk.

Using an OFFLINE LICENSE FILE on the CLI

On the **DATA RECON** CLI, selecting the **Use offline license file** option will prompt you to locate your OFFLINE LICENSE FILE on the disk.



If the license file you are using is outdated, or if it does not contain the appropriate license for the TARGET that you wish to scan, **DATA RECON** will prompt you to authenticate online.

Placing the OFFLINE License File in the Same Folder as the DATA RECON Executable

The **DATA 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.

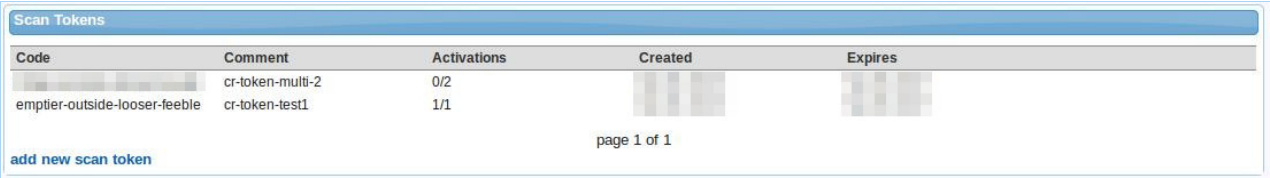
If it does not, **DATA RECON** will prompt you to authenticate online.

GENERATING AND USING SCAN TOKENS

SCAN TOKENS are easy-to-remember passphrases that can be distributed to authorized users.

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

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



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

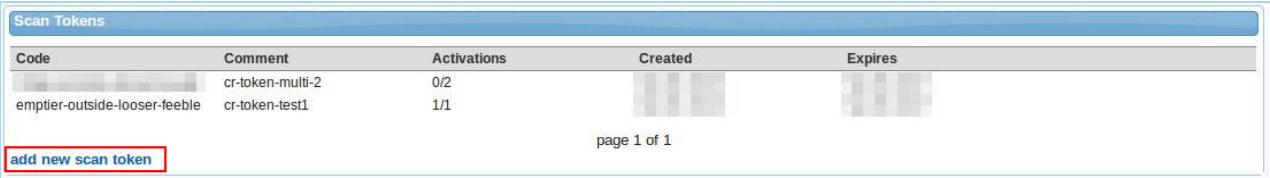
This allows users other than the owner of the Ground Labs Services Portal account to (among other things):

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

GENERATING SCAN TOKENS

Generate SCAN TOKENS at the Ground Labs Services Portal dashboard.

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



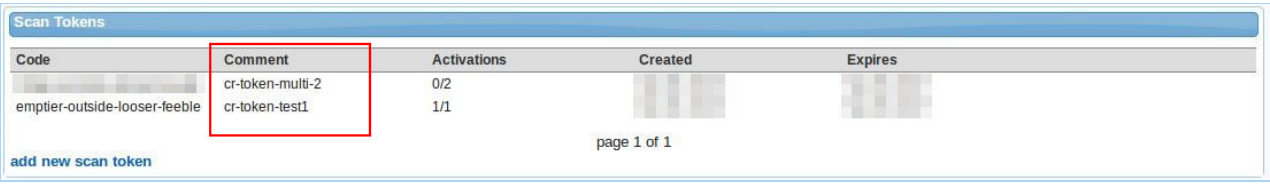
Clicking on "add new scan token" will bring up its dialog window.

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

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

Identifying Scan Tokens

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



Comments can be used to help document:

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

Note: Make sure that you're selecting the correct license source that you want to associate the SCAN TOKEN(S) with.

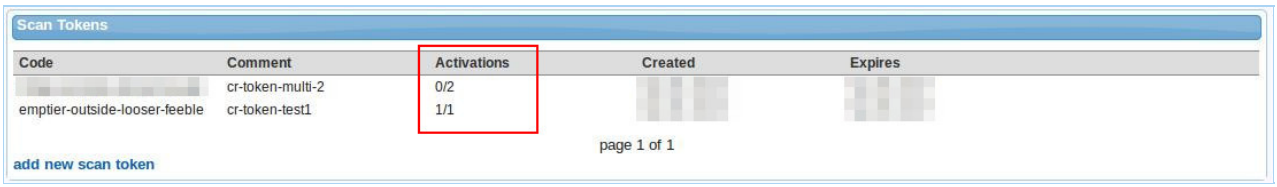
USING AND ACTIVATING SCAN TOKENS

A SCAN TOKEN has a "license source" it is attached to.

A "license source" is the pool of licenses that the SCAN TOKEN can draw from when assigning licenses to new TARGETS.

A SCAN TOKEN can be used to log into an instance of **DATA RECON** without assigning a license to the host.

When attempting to scan a new TARGET while logged into **DATA RECON** using a SCAN TOKEN, **DATA RECON** will draw from the "license source" that is attached to the SCAN TOKEN it is using to assign the a license to the new TARGET.



SCAN TOKENS are not "activated" when used to log into **DATA RECON**.

They are "activated" when, after logging into **DATA 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 **DATA 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 **DATA 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, **DATA 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 **DATA RECON**.

But when that login instance is used to attempt a scan on TARGET **DATA 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 **DATA RECON**. A license is only assigned when a SCAN TOKEN is used to log into a copy of **DATA 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 DATA RECON

DATA RECON configuration can be done through either the

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

DATA RECON GRAPHIC USER INTERFACE

DATA RECON is typically configured through the **DATA RECON** Graphic User Interface (GUI) on Windows.

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

You can configure **DATA RECON** through the following options on the **DATA RECON** GUI dashboard:

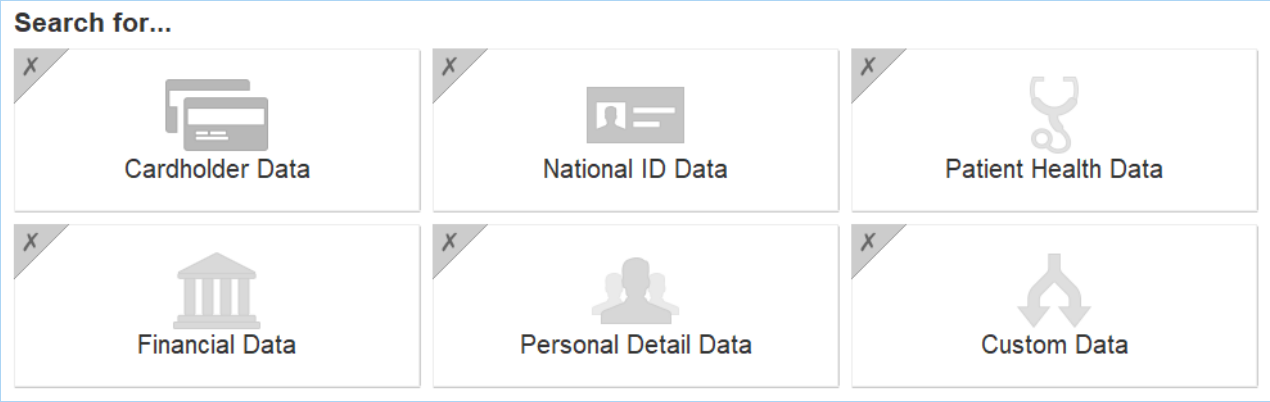
- Selecting Match Patterns
- Selecting Target Location
- Setting Resource Usage
- Setting Credentials for Restricted Targets
- Setting Custom Search Rules
- Setting Results Database Options
- Setting Compliance Report Savings Options

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

Note: You can log into **DATA RECON** using your Ground Labs Services Portal user name and password or a SCAN TOKEN without needing to validate a license.

SELECTING MATCH PATTERNS

The **DATA RECON** dashboard allows you to build a search query to find data security risks.



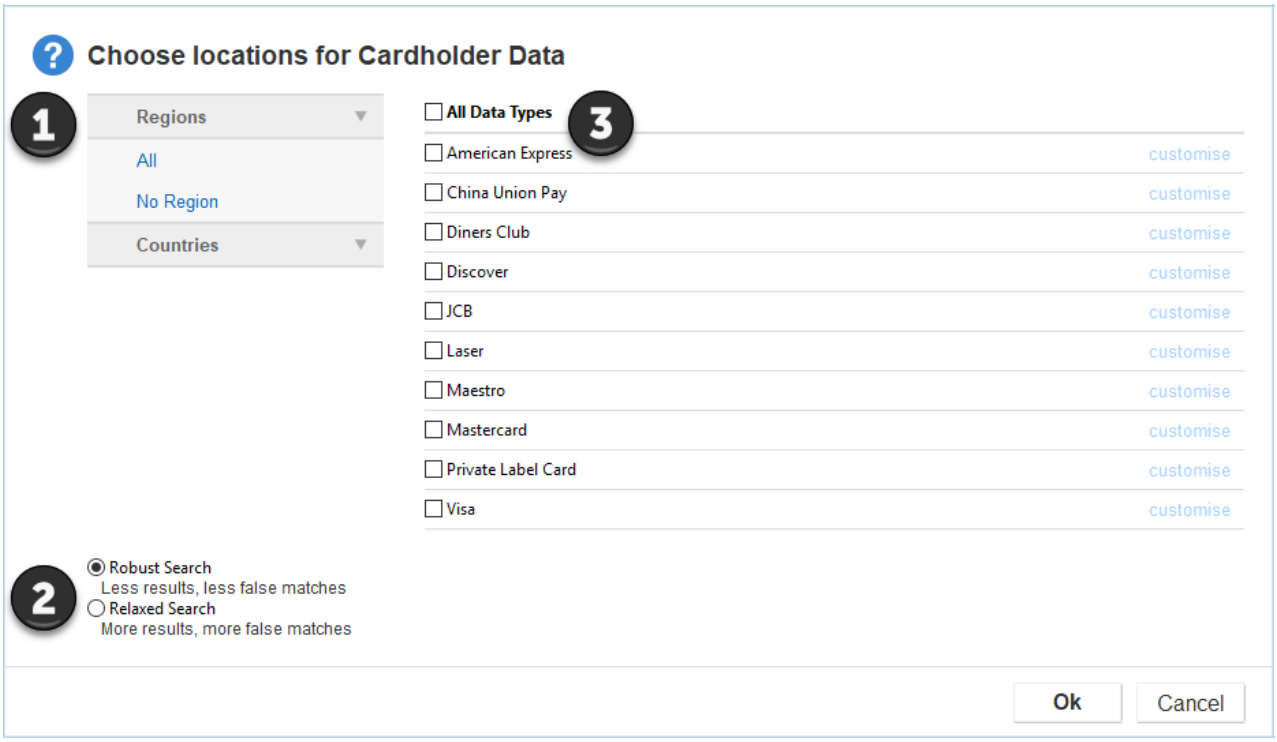
You can scan for 5 categories of predefined data types:

Data Type	Description
Cardholder Data	Cardholder data from ten major card brands; also checks for test numbers, track type 1 and track type 2 magnetic stripe data.
National ID Data	More than 50 types of National IDs, including Social Security Numbers (SSNs) and Tax File Numbers (TFNs) from most of Africa, Asia, Europe, Middle East, Oceania, North America and South America.
Patient Health Data	Patient Health Information (PHI), including Medicare, National Insurance and National Provider Identifier data types from multiple regions.
Financial Data	Sensitive finance-related data, including business/company registration details and bank account numbers.
Personal Detail Data	Personal names, addresses, and other Personally Identifiable Information (PII). You can build your own match pattern data types with the "Custom Data" option, or customize existing match pattern data types to suit your own search needs.

MATCH PATTERN OPTIONS

When you click on a match pattern data type category, the match pattern options dialog for that data type category is displayed. Match pattern options let you build search options from a set of five predefined match pattern data types.

Clicking on a match pattern data type category on the **DATA RECON** GUI dashboard displays a new dialog that asks you to **Choose locations for <match pattern type>**.



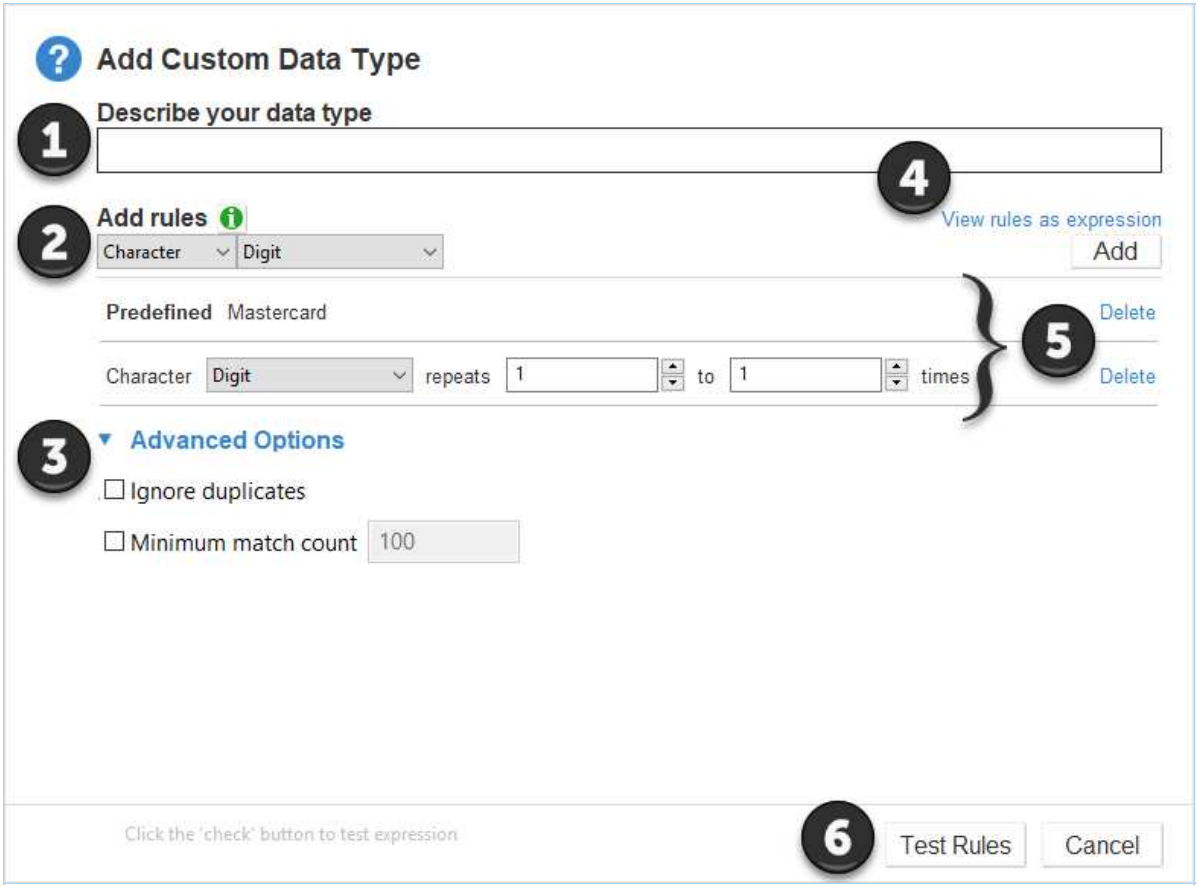
Label		Description
1	Regions/Countries	When you select the match pattern data types that you want to search for, **DATA RECON** shows the regions or countries that your data types cover. **Note:** Searching for match pattern types from 3 or more geographic regions will produce unusually high rates of duplicate results and false positives. Run separate scans when searching for sensitive data from different regions for more accurate results.
2	Robust/Refined Search	• **Robust Search**: Strict search on selected match pattern data types, with fewer results and a lower rate of false positives. • **Refined Search**: Broader search on selected match pattern data types, with greater number of hits and a higher rate of false positives. **Tip:** It is recommended that you use the **Robust Search** option, especially for these match pattern data types: US Routing Transit Number, Australian Medicare Provider, UK Community Health Index, License Number, Login Credentials.

CREATE CUSTOM DATA

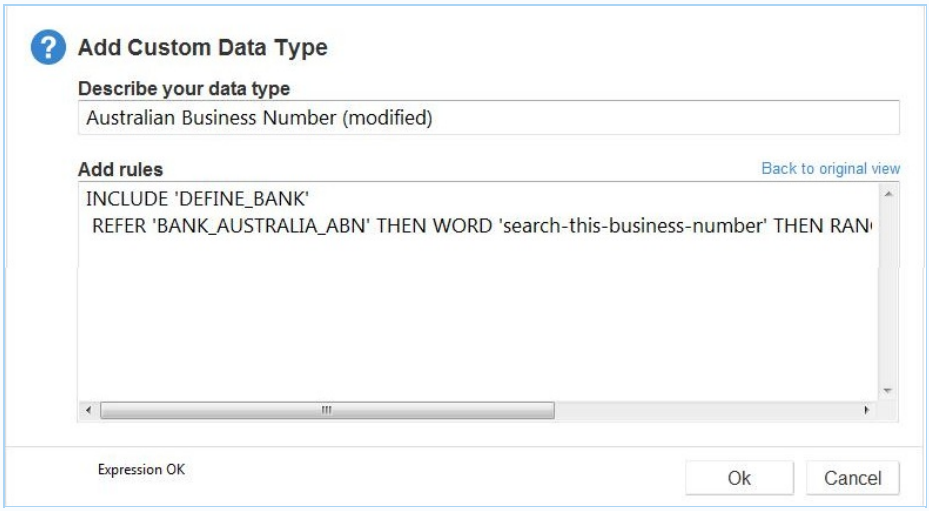
You can build custom match pattern data types in the **DATA RECON** GUI to make your scans more specific.

1. On the **DATA RECON** GUI dashboard, select the **Custom Data** match pattern data type category.

2. Select a data type from one of the predefined match pattern data type categories and click **Customize**.
3. In the **Add Custom Data** dialog, do the following:



Field		Details
1	Describe your data type	Enter the name for you custom match pattern data type.
2	Add Rules	See Add Rules.
3	Advanced Options	Select where applicable: ◦ **Ignore duplicates**: Ignores duplicate matches found by this custom data type. ◦ **Minimum match count**: Only report matches found by this custom data type if the number of matches found meets the minimum match count specified.

Field		Details
4	View rules as expression	Displays show the search expression that the selected search rules produce for the custom data type. You can edit the search expression using this option. 
5	Rule list	Displays list of search rules that you have added
6	Test Rules/Ok	After you add rules to the custom data type, click **Test Rules** to validate your scan rule. Once **DATA RECON** validates your custom data type, the **Test Rules** button changes into an **Ok** button. To add the scan rule, click **Ok**.

Add Rules

You can add 3 types of search rules to your custom data type:

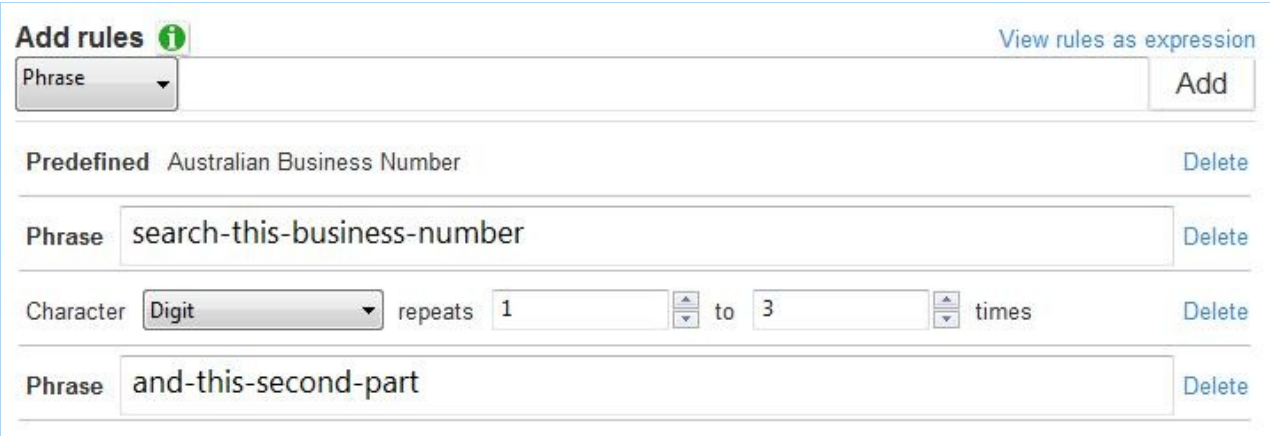
Search Rule	Description
PREDEFINED	Only searches within a given predefined match pattern data type from one of the categories of data types. **Example:** When you select "Australian Business Number", it only runs a search within the "Australian Business Number" predefined match pattern data type.
PHRASE	Searches for a specific phrase or string of characters. Certain characters such as the single quote ', double quote ", and the backslash \ cannot be used in **Phrase**, and will not form a legal search expression.

Search Rule	Description
CHARACTER	Adds a character to your search string, and behaves like a wild card character (*). Wild card characters are used to search for strings containing characters that meet certain parameters. **Example:** Adding a "Character" rule "Digit" that repeats 1 - 3 times matches: 123, 587 and 999. However, it does not match: 12b, !@#, foo **Character** allows you to pick these options to add as character search rules to match: • **Space**: Any whitespace character. • **Alphanumeric**: Numerical characters and letters. • **Alphabet**: Any character from the alphabet. • **Digit**: Any numerical character. • **Printable**: Any printable ASCII character, including vertical whitespace. • **Sameline**: Any printable ASCII character, excluding vertical whitespace. • **Graphic**: Any ASCII character that is not whitespace or a control character. • **Non-alphanumeric**: A symbol that is neither a number nor a letter; e.g. apostrophes ‘, parentheses (), brackets [ ], hyphens -, periods ., and commas ,. • **Non-alphabet**: Any non-alphabet characters; e.g. ~ ` ! @ # $ % ^ & * ( ) _ - + = { } | [ ] : ; " ' < > ? / , . • **Non-digit**: Any non-numerical character.

Rules Resolution

Search rules resolve from top to bottom (as arranged on the GUI), or from left to right (in the search expression).

Example



DATA RECON resolve the custom data type search rules in the following order:

1. **Predefined**: Australian Business Numbers.
2. **Phrase**: search-this-business-number.
3. **Character**: Digit that repeats 1 - 3 times.
4. **Phrase**: and-this-second-part.

The resulting search expression is as follows:

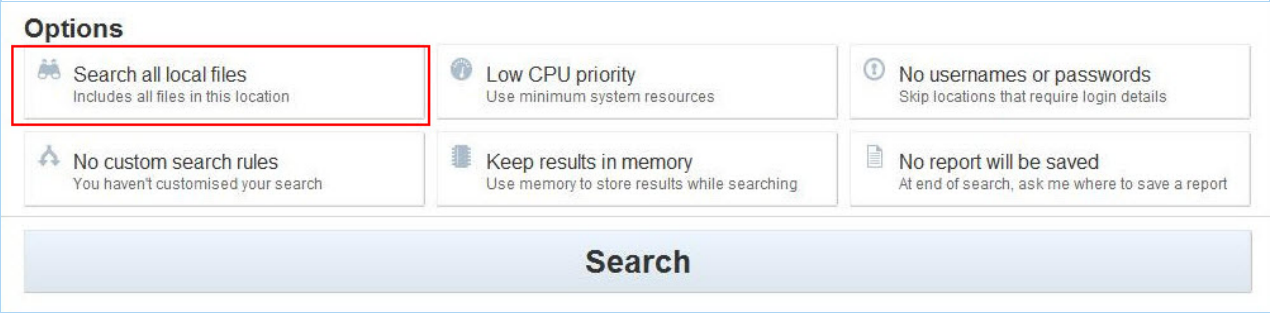
```
INCLUDE 'DEFINE_BANK'

REFER 'BANK_AUSTRALIA_ABN' THEN WORD 'search-this-business-number'
THEN RANGE DIGIT TIMES 1-3 THEN WORD 'and-this-second-part'
```

DATA RECON will search for the following string in the next scan:

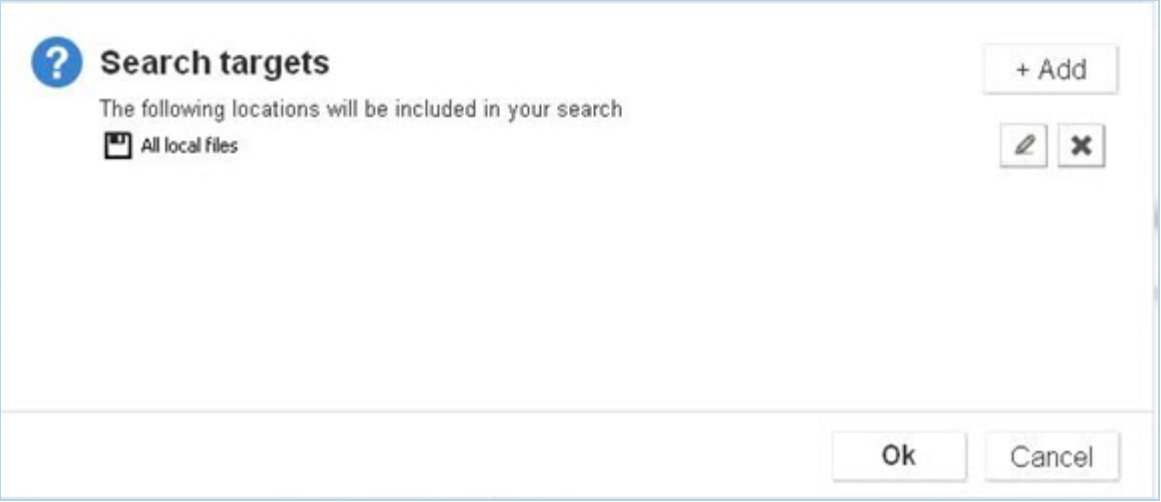
```
<Australian Business Number>+search-this-business-number+***+and-this-second-p
art
```

SELECTING TARGET LOCATION

You can select search locations with the **DATA 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.



DATA RECON can scan the following TARGET types for sensitive data:

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

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 **DATA RECON** Licensing.

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

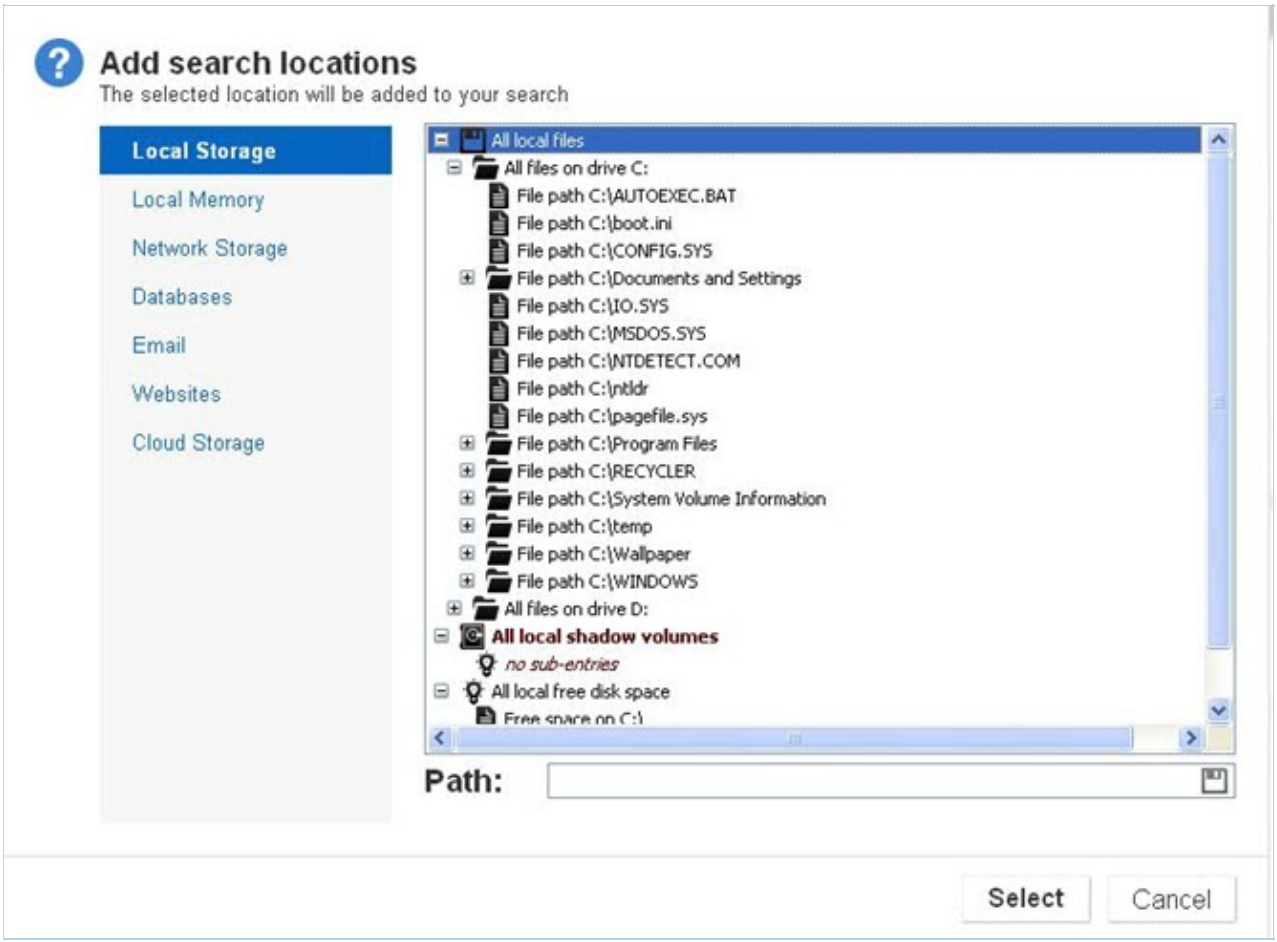
LOCAL STORAGE

DATA 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 **DATA 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
- All local shadow volumes
- All local free disk space

ALL LOCAL FILES

By default, DATA 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

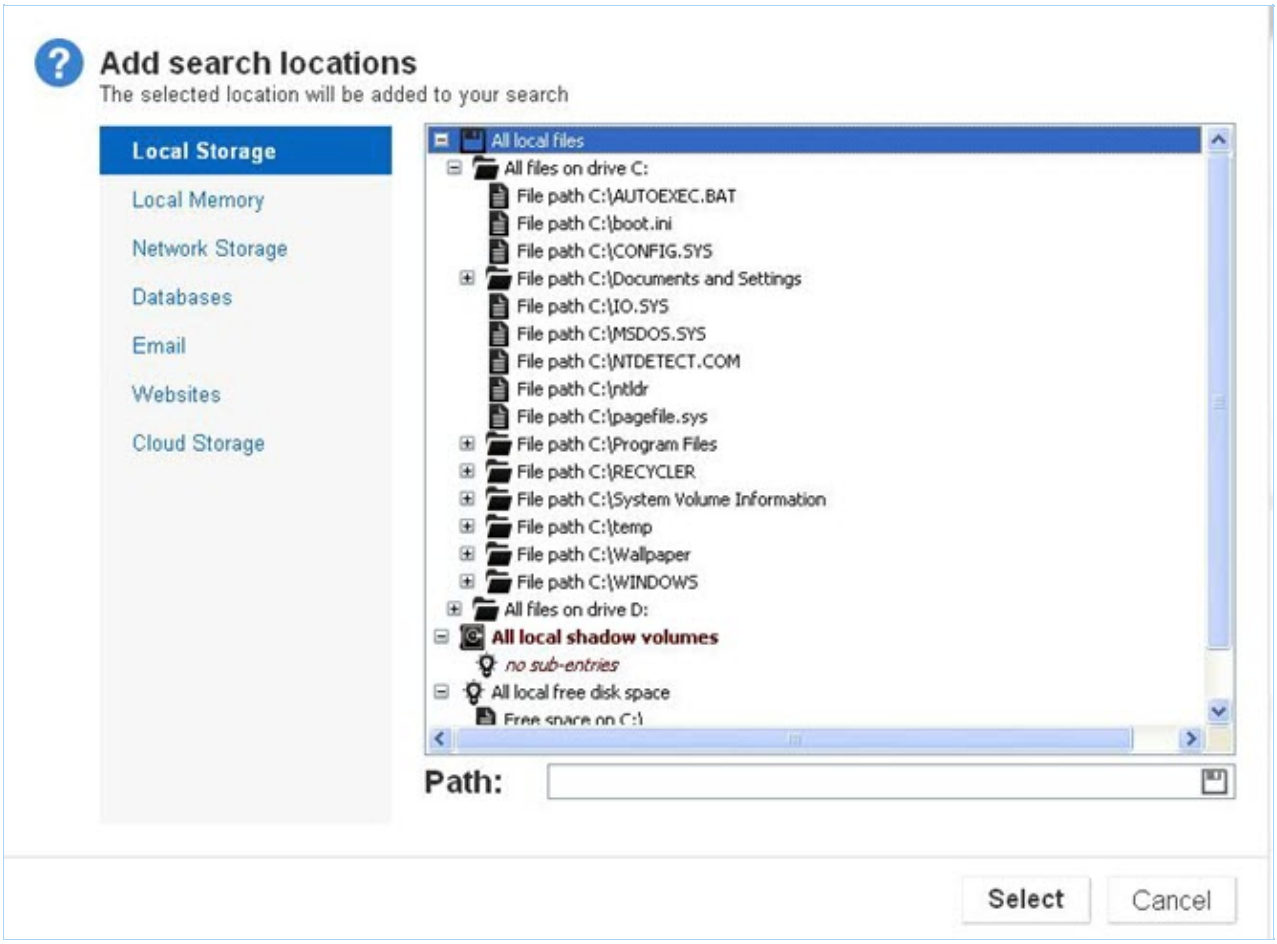
ALL LOCAL FREE DISK SPACE

(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

DATA 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

DATA RECON can scan network storage media for sensitive data.

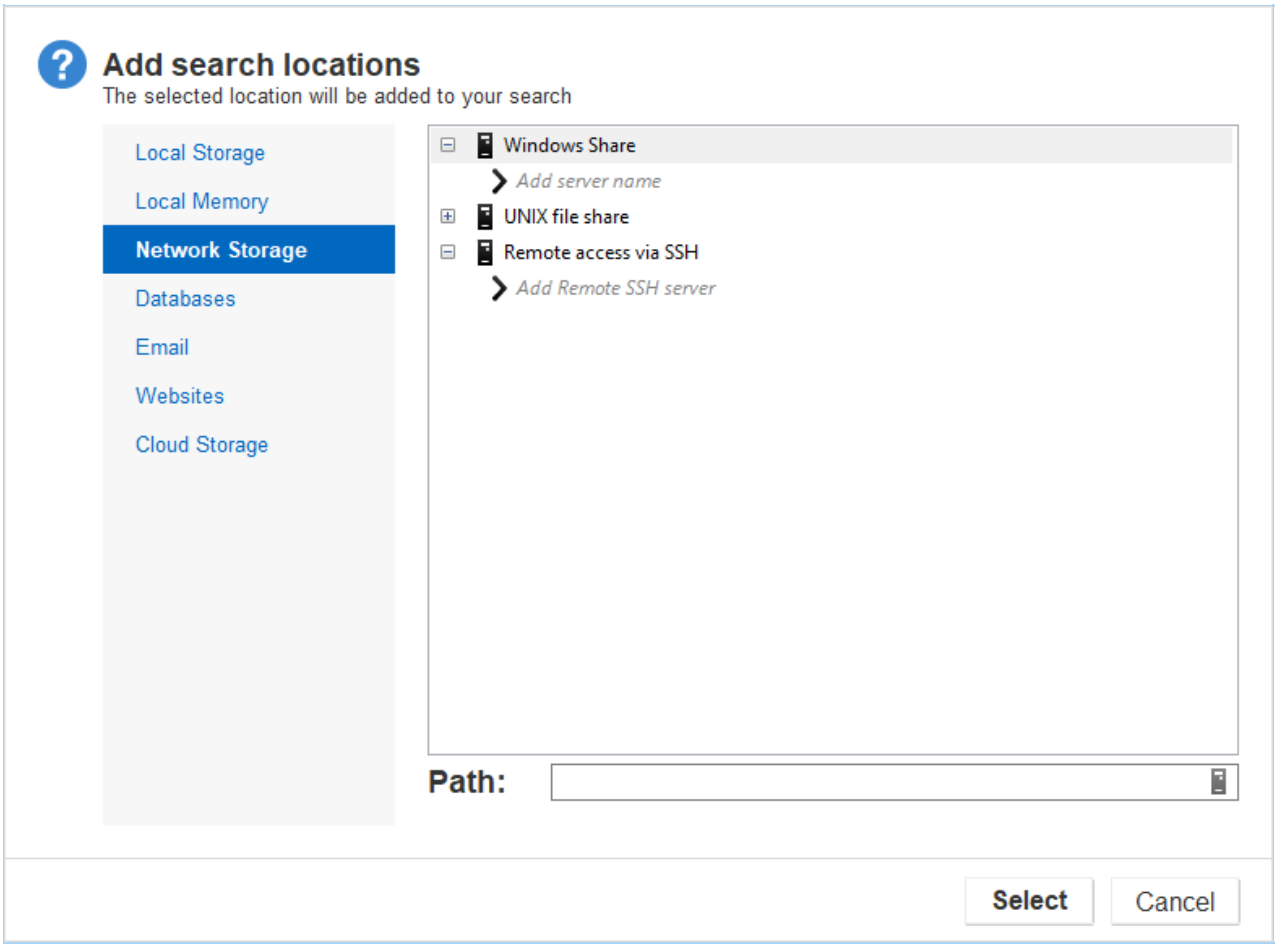
This would include being able to scan remote file servers, Storage Area Networks (SAN) devices, and Network-Attached Storage (NAS) devices.

You can scan scan the following Network Storage types:

- Windows Share
- UNIX File Share
- Remote Access via SSH

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

To avoid increasing your PCI footprint and network slowdowns, run a Local Storage scan instead.



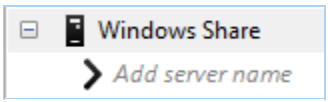
WINDOWS SHARE

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

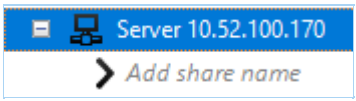
DATA RECON displays the Windows shares available on the network. You can also add a Windows share TARGET by typing the host name or IP address of a Windows share

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.



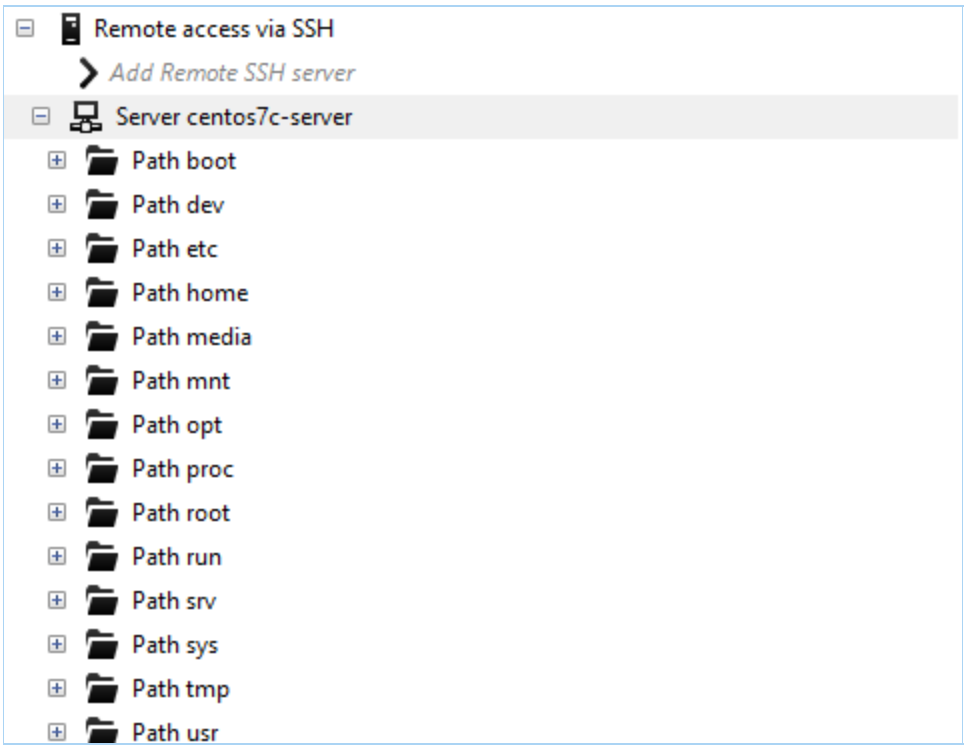
UNIX FILE SHARE

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

DATA 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
- Live Database Scan

FILE-BASED SCAN

(Not recommended) The data storage files of a database can be scanned directly. Performing a Local Storage 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	• **DATA RECON** Advanced Edition
Microsoft SQL Server 2005 and above	• **DATA RECON** Advanced Edition
PostgreSQL 9.5 and above	• **DATA RECON** Advanced Edition
Oracle Database 9 and above	• **DATA RECON** Advanced Edition • Oracle Instant Client installed on host
IBM DB2 11.1 and above	• **DATA RECON** Advanced Edition • Data Server Driver for ODBC and CLI installed on host

Database	Requirements
Sybase/SAP Adaptive Server Enterprise (ASE) 15.7 and above	• **DATA RECON** Advanced Edition • Sybase/SAP ASE installed on host

Remediating Matches

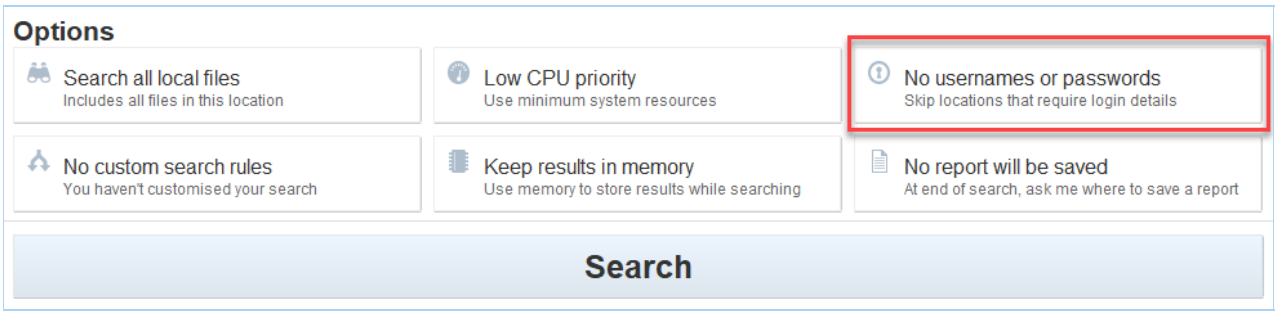
DATA RECON does not modify data in the databases it scans. As a result, direct remedial action is unavailable for matches found in a live database scan.

You can, however, mark matches for manual remedial action. See Remediating and Marking Matches 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:

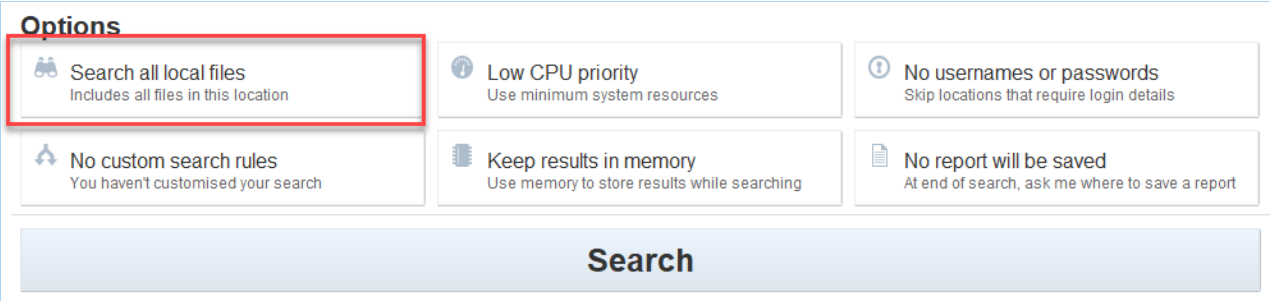
1. Click **+ Add** and select one of the following:
    - **MySQL**
    - **Oracle**
    - **Microsoft SQL**
    - **IBM DB2**
    - **PostgreSQL**
    - **Sybase**

2. Fill in the following fields:
    - **Target location**: Enter the database server hostname.
    - **Username**: Enter your user name.
    - **Password**: Enter your password.

    > **Tip:** Credentials are only saved if:
    > - Search configuration is saved. See Save and Load Options for more information.
    > - The results database is saved. See Setting Results Database Options for more information.
3. (optional) Under **Encrypt credentials** enter a master password to encrypt stored credentials.
4. Click **Ok**.

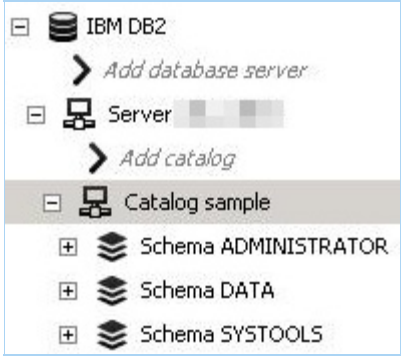
Add Databases to Search Locations

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 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

Database	Connection Options

Oracle Database	**Connect using a fully qualified domain name (FQDN)**
	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.
	Oracle 12x/TNS: protocol adapter error
	If you are using Oracle 12x, or if the Oracle database displays a "TNS: protocol adapter error", you must specify a `SERVICE_NAME`.
	Add the service name to the database server host name:
	`<hostname(SERVICE_NAME=<SID>)[:port]>[/catalog[/table]]`
	For example:
	`db_server(SERVICE_NAME=GLAB)/catalog_A/table_1`

Microsoft SQL Server	Scan a specific SQL Server instance (where multiple are running):
	`<hostname(instance=<instance_name>)[:port]>`
	For example:
	`db_server(instance=mssql_instance_1)`

Sybase/SAP ASE	Scan a specific Sybase instance (where multiple are running):
	`<hostname(instance=<instance_name>)[:port]>`
	For example:
	`db_server(instance=sybase_instance_1)`

EMAIL

DATA RECON can scan the following email locations:

- Google Mail (IMAP)
- Office 365 Mail (IMAP)
- Internet Mailbox
- Internet SSL Mailbox
- IBM Notes
- Locally Stored Email Data

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 or Internet SSL Mailbox (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)

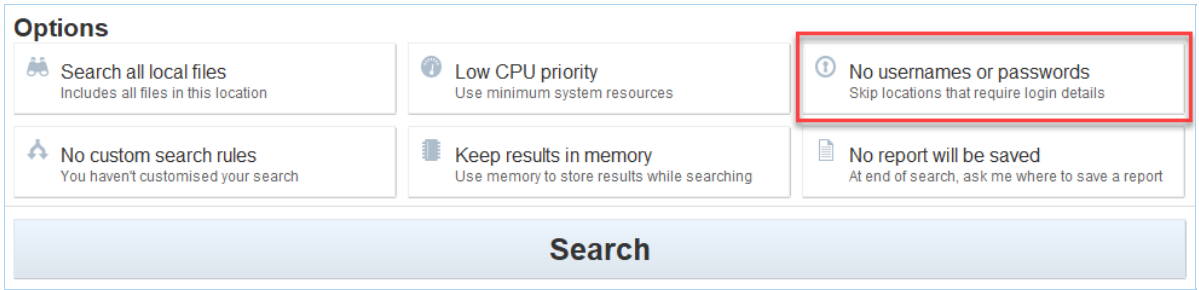
Requirements

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**.



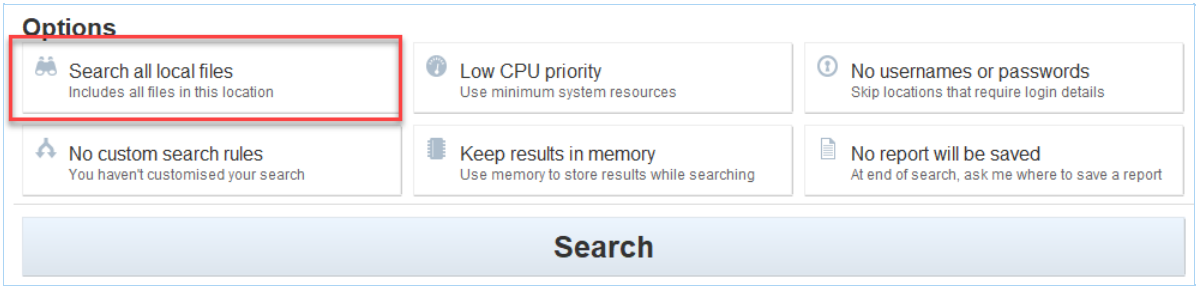
2. In the **Search target credentials** dialog box, click **+ Add** and select **Google Mail**.
3. Fill in the fields:
   - **Target location**: Enter the target mailbox as `<domain/email_address>`. For example, if the target mailbox resides on the domain `example.com` at address `user@example.com`, 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 two-factor authentication (2FA) enabled, create an app password and enter it here. See Two-factor Authentication (2FA) 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.

Two-factor Authentication (2FA)

To access Google Mail accounts with two-factor authentication (2FA) 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. Click on **Select app**, select **Other (Custom name)** and enter "Scan". Click **GENERATE**.
5. In the "App passwords" page, go to the **Select the app and device for which you want to generate the app password** section.
6. Google then displays a 16 character “App password”. Use the app password in place of your Google Mail password when entering credentials into DATA RECON.

OFFICE 365 MAIL (IMAP)

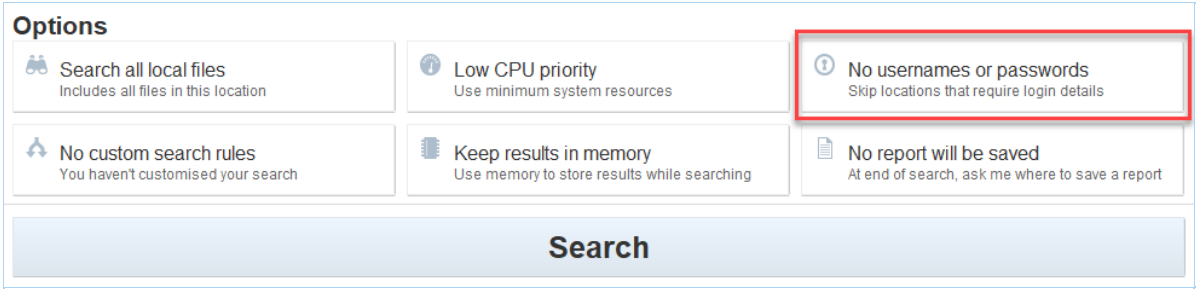
Requirements

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 two-factor authentication (2FA) enabled, create an app password and enter it here.

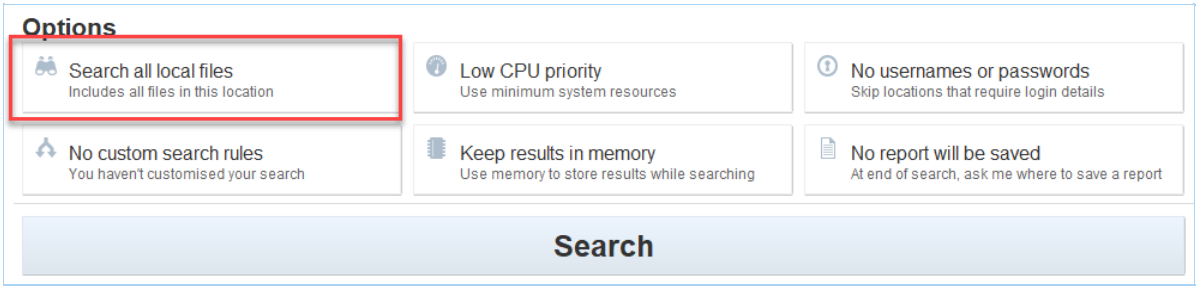
     > **Info: Two-factor Authentication**
     > If you have two-factor authentication enabled for your Office 365 account, you must create an app password for use with **DATA RECON**. See Microsoft: Manage app passwords for two-step verification for more information.

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 **DATA RECON** and the mail server encrypted. See Internet SSL Mailbox 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 Target allows you to add general email accounts as Targets.

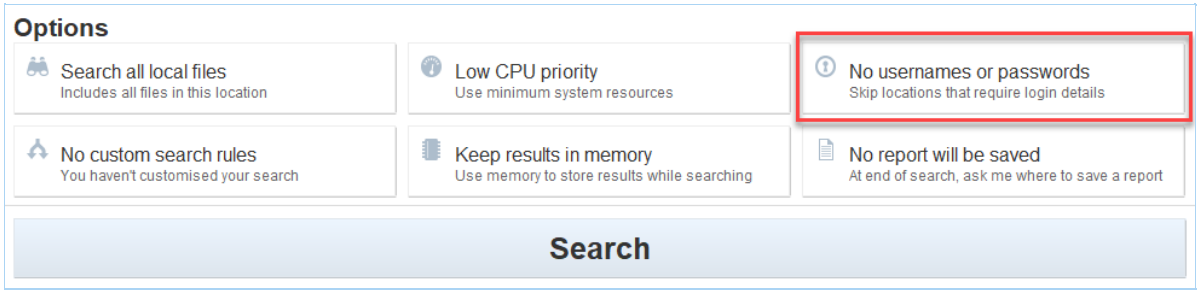
To add a general email account as an Internet Mailbox Target, the email account must:

- 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 two-factor

authentication (2FA) enabled, create an app password and enter it here.

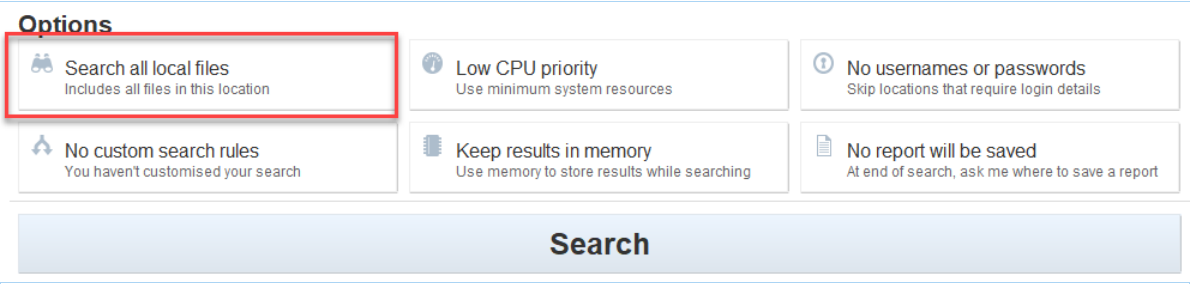
> **Info: Two-factor Authentication**
> Two-factor authentication is not supported. To access Internet Mailbox accounts that require two-factor authentication, you must set up an app password for use with **DATA RECON**. Create and use the app password instead of your account password.

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 Target allows you to add general email accounts as Targets.

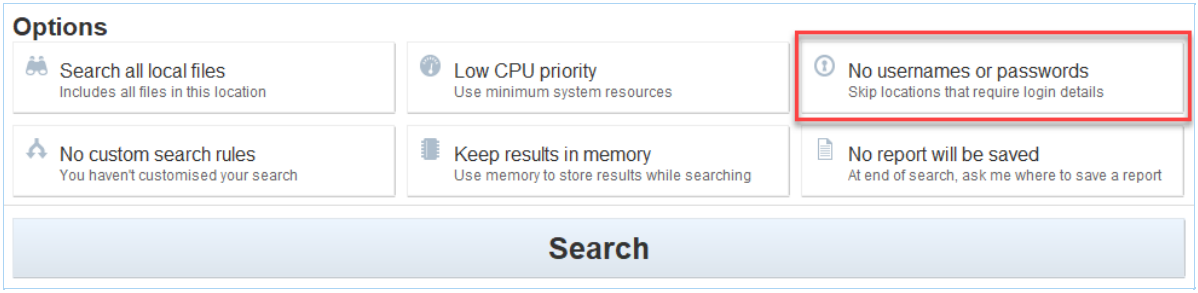
To add a general email account as an Internet SSL Mailbox Target, the email account must:

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

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 two-factor authentication (2FA) enabled, create an app password and enter it here.

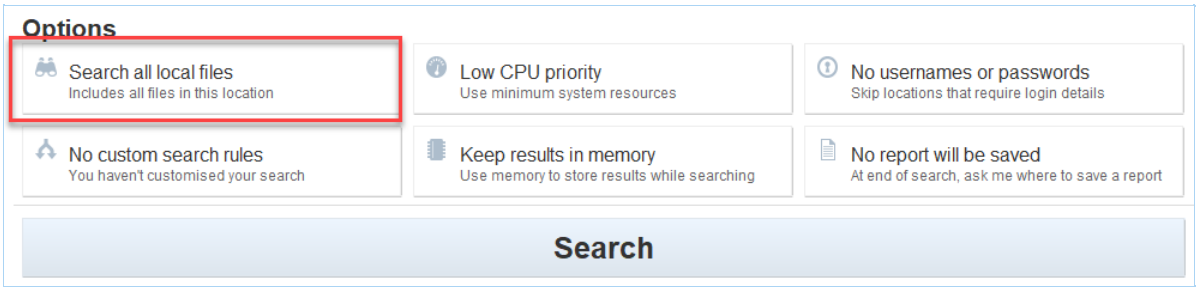
     > **Info: Two-factor Authentication**
     > Two-factor authentication is not supported. To access Internet SSL Mailbox accounts that require two-factor authentication, you must set up an app password for use with **DATA RECON**. Create and use the app password instead of your account password.

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.

IBM NOTES

Requirements

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

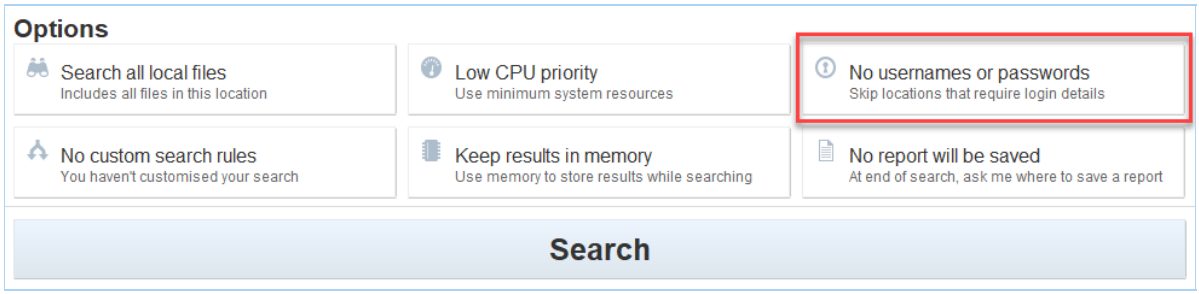
Supported IBM Notes clients:

- IBM Notes client 8.5.3
- IBM Notes client 9.0.1

Add Credentials

Add credentials for the IBM Notes Target:

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

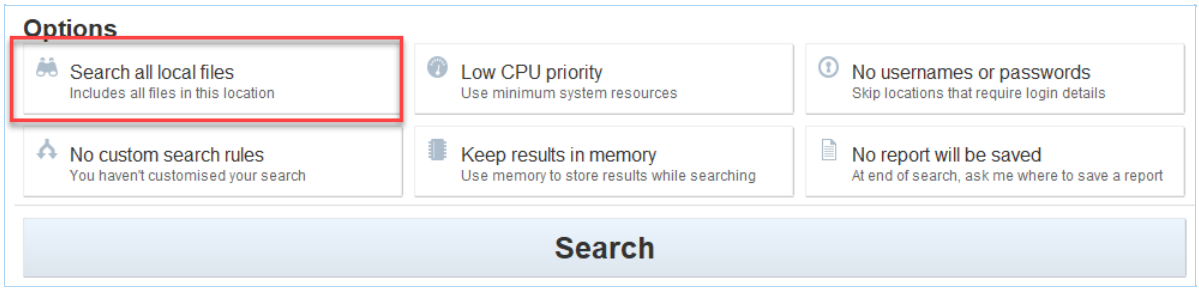


2. In the **Search target credentials** dialog box, click **+ Add** and select **.
3. Fill in the fields:
   - **Target location**: Enter the IBM Domino server domain name.
   - **Username**: Your Notes User Name.
   - **Password**: Enter the user's password.
4. (Optional) Enter a password under **Encrypt credentials** to encrypt the saved credentials.
5. Click **Ok**.

Add Search Location

Add a IBM Notes account as a search location:

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



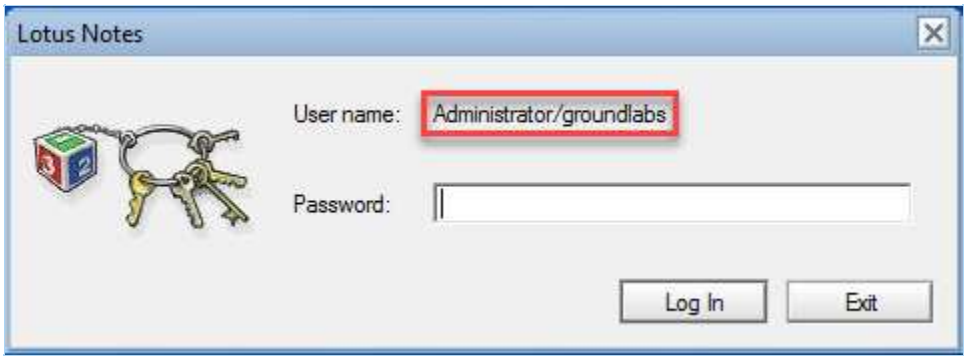
2. In the **Search targets** dialog box, click **+ Add** and select **Email**.

3. Select and expand **IBM Notes**.
4. Enter your IBM Domino server domain and press enter.
5. Select the "Domain" Target that appears.
6. (Optional) Select individual folders and emails to scan.
7. Click **Select** to finish adding the IBM Notes Target.

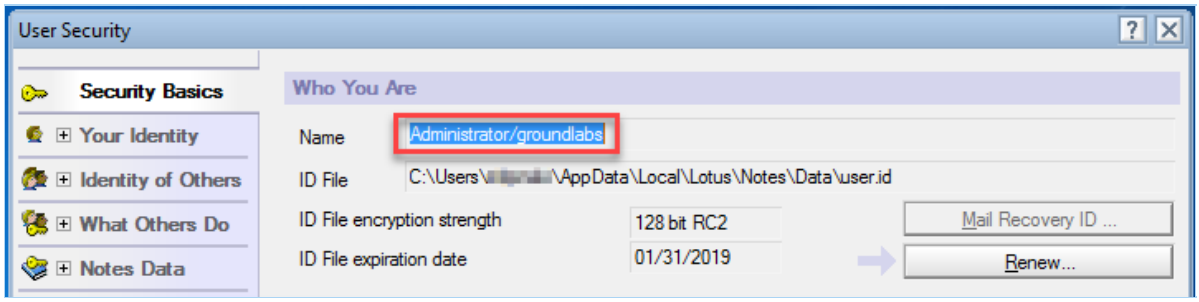
Notes User Name

To find your Notes user name:

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



4. If no password prompt opens, find your 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 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 scan. 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 scan on the backup information store files.

WEBSITES

DATA RECON can crawl the contents of a given website to search for sensitive data. **DATA 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 in 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 applicable.
3. Enter your credentials. Click **Ok** to save your credentials.

WEBSITE SEARCH OPTIONS

DATA RECON allows you to modify your website searches.

Maximum Search Depth

The "maximum search depth" limits the link-depth that **DATA 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 **DATA RECON** from endlessly crawling links on the given website.

Follow External Website Links

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 **DATA RECON**:

- Azure Storage
- Google Apps
- Rackspace Cloud

RACKSPACE CLOUD

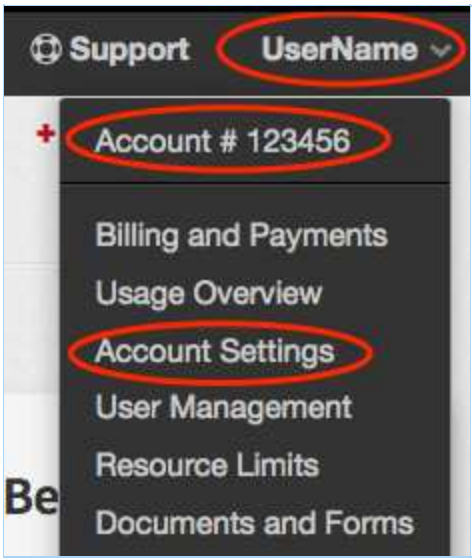
Support for Rackspace services is currently limited to Cloud File Storage only.

To add Rackspace Cloud File Storage as a cloud Target:

1. Get Rackspace API Key
2. Add Credentials
3. Add Target

GET RACKSPACE API KEY

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

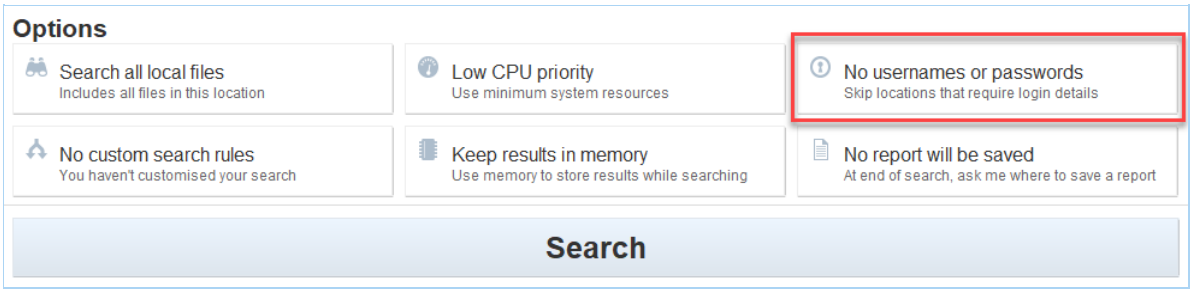


3. In the **Account Settings** page, go to **API Key** and click **Show**.

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

ADD CREDENTIALS

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

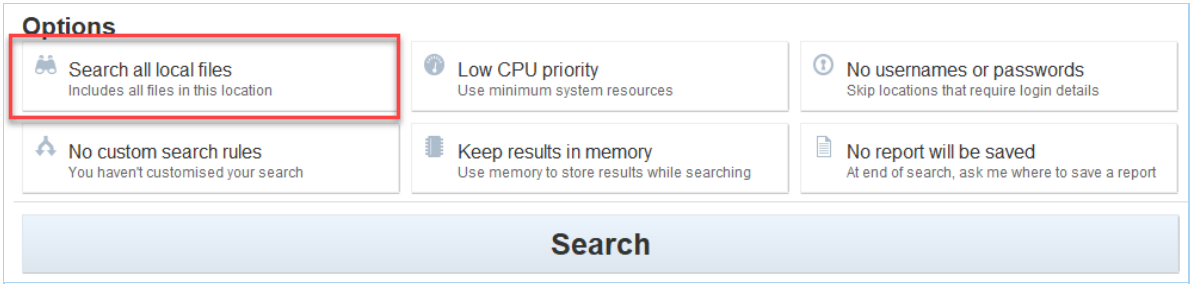


2. In the **Search target credentials** dialog box, click **+ Add** and select **Rackspace Cloud Files (HTTPS)**.
3. Fill in the following fields:
    - **Target location**: Enter the Rackspace account name.
    - **Username**: Enter the Rackspace account name.
    - **Password**: Enter the API key obtained in Get Rackspace API Key.
4. (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 for more information.
    - The results database is saved. See Setting Results Database Options for more information.
5. Click **Ok**.

ADD TARGET

1. In the main menu, click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and 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 Cloud Files 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 Rackspace Target.

GOOGLE APPS

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

- Google Drive
- Google Tasks
- Google Calendars

To add Google Apps as cloud Targets:

1. Configure Google Apps Account
2. Add Credentials
3. Add Target

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.

To configure your Google Apps account for scanning:

1. Select a project
2. Enable APIs
3. Create a Service Account
4. Set up Domain-Wide Delegation

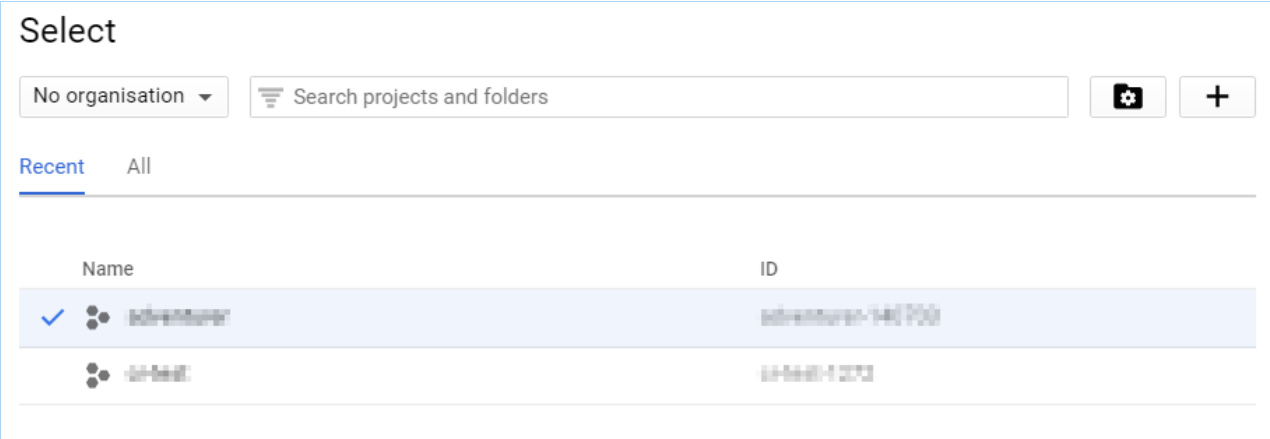
Info: Setting up a Google Apps account as a Target location requires more work than other cloud services because the Google API imposes certain restrictions on software attempting to access data on their services. This keeps their services secure, but makes it more difficult to scan them using **DATA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

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.



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:

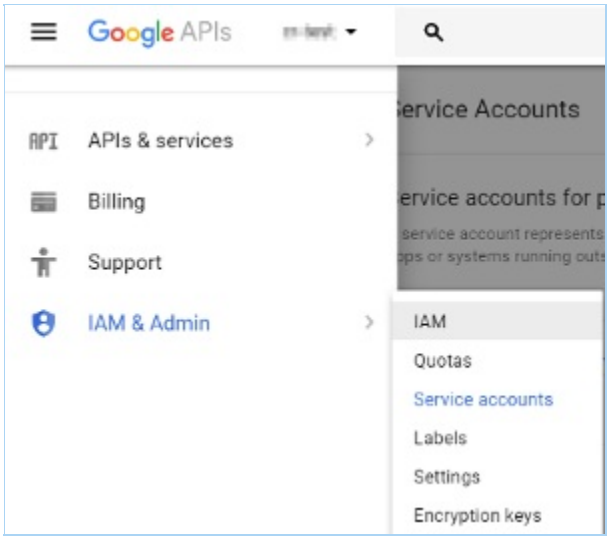
1. Select a project.
2. In the project Dashboard, click **+ ENABLE APIS AND SERVICES**. This displays the API Library.
3. Enable the **Admin SDK** API.
   a. Under G Suite APIs, click **Admin SDK**.
   b. Click **ENABLE**.
4. Repeat to enable the following APIs:

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

Create a Service Account

Create a service account for **DATA 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**.

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

Field	Description
Service account name	Enter a descriptive label.
Role	**Select Project** > **Owner**.
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: `service-account-634@project_name-1272.iam.gserviceaccount.com`
Furnish a new private key	1. Select **Furnish a new private key**. 2. Select **P12**.
Enable G Suite Domain-wide Delegation	Select **Enable G Suite Domain-wide Delegation**.

> **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: "**DATA 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`. **DATA 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

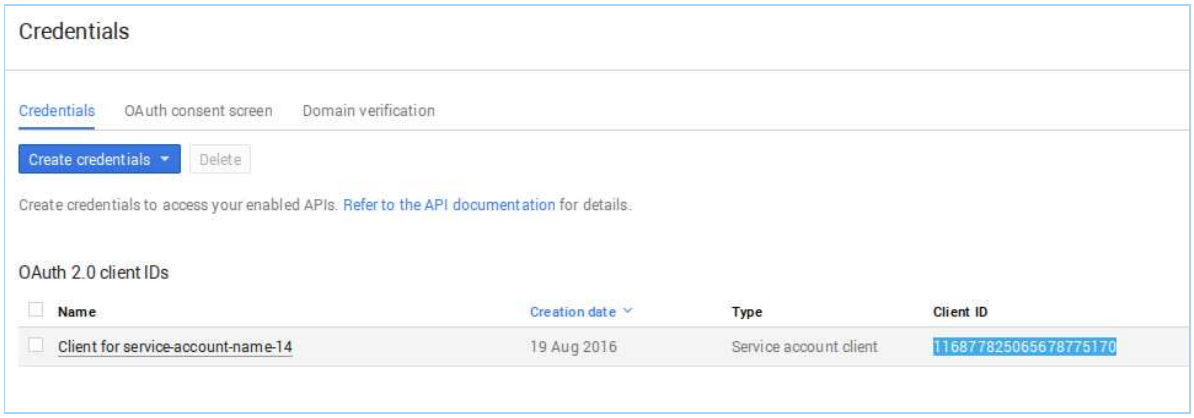
> **Note:** Set up domain-wide delegation with the administrator account used in Enable APIs.

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

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

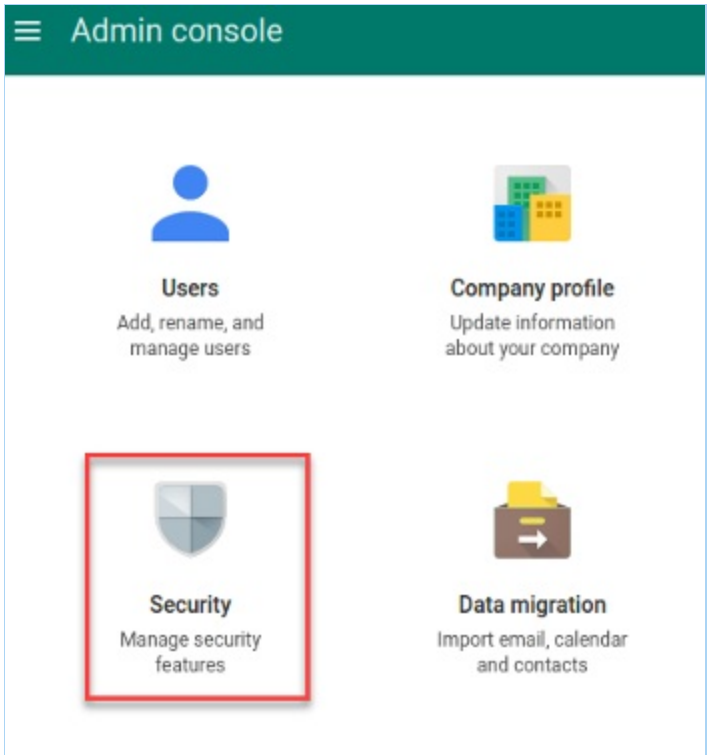
To set up domain-wide delegation:

1. Click on the ☰ menu on the upper-left corner of the Google Developers Console.
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**.

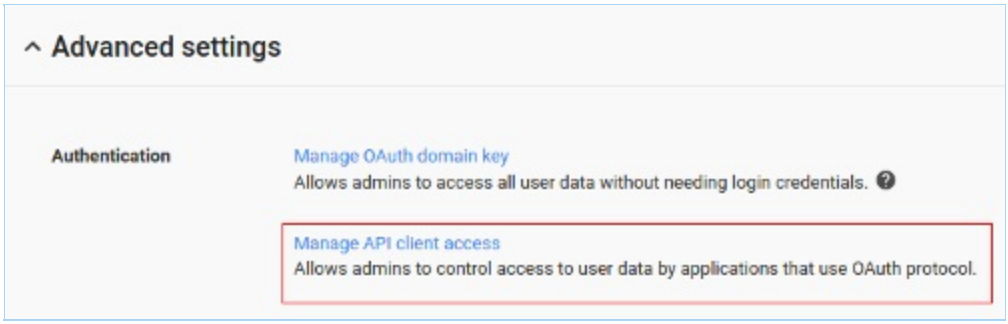


Note: The Client ID is required when assigning DwD to your Service Account.

4. Go to the Google 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**.



8. In **Manage API client access**, enter:
   a. **Client Name**: Your Service account **Client ID** (For example, `116877825065678775170`).
   b. **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 **DATA RECON** to work with each Google Apps service:

Google Apps service	API Scope
All (required)	`https://www.googleapis.com/auth/admin.directory.user.readonly`
Google Drive	`https://www.googleapis.com/auth/drive.readonly`
Google Tasks	`https://www.googleapis.com/auth/tasks.readonly`
Google Calendar	`https://www.googleapis.com/auth/calendar.readonly`

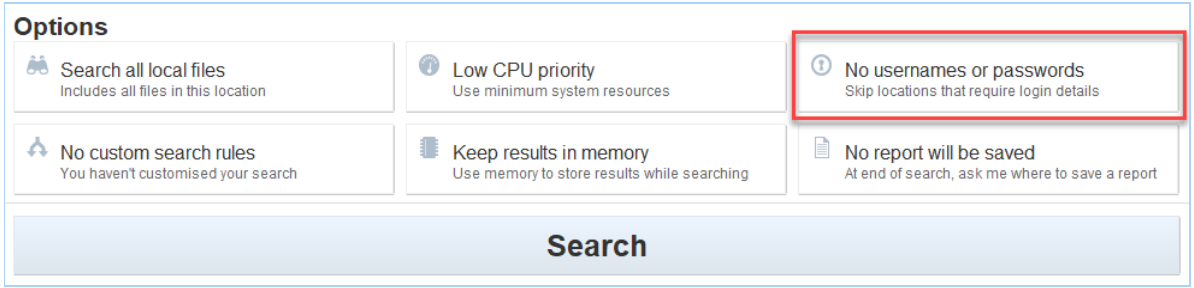
> **Info:** You can apply multiple API Scopes by separating them with commas. For example,
>
> `https://www.googleapis.com/auth/admin.directory.user.readonly, https://www.googleapis.com/auth/drive.readonly`

> **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

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



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

instructions below carefully.

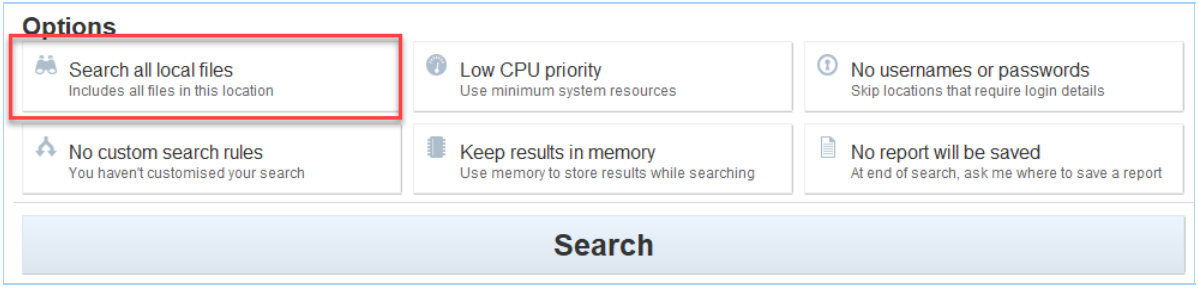
2. In the **Search target credentials** dialog box, click **+ Add** and select one of the following Target types:
   - **Google Docs**
   - **Google Tasks**
   - **Google Calendars**
3. Fill in the following fields:
   - **Target location**: Enter the Google Apps domain.
   - **Username**: Enter a Google Apps domain administrator email address.

     Note: Use the same administrator account used to Enable APIs and Set up Domain-Wide Delegation.
   - **Password**: Leave blank.
4. Click **+ Add** again, and select the same Target type.
5. 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. The P12 key must be saved in the same folder as the **DATA RECON** executable.
6. (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 for more information.
   - The results database is saved. See Setting Results Database Options for more information.
7. Click **Ok**.

ADD TARGET

1. In the main menu, click on **Search all local files**.



2. In the **Search targets** dialog box, click **+ Add** and select **Cloud Storage**.
3. Select one of the following and click **+** to expand the selection:
   - **Google Drive**
   - **Google Tasks**
   - **Google Calendars**
4. 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`.

5. Press **Enter** to add the specified Google Apps domain 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 Google 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
2. Add Credentials
3. Add Target

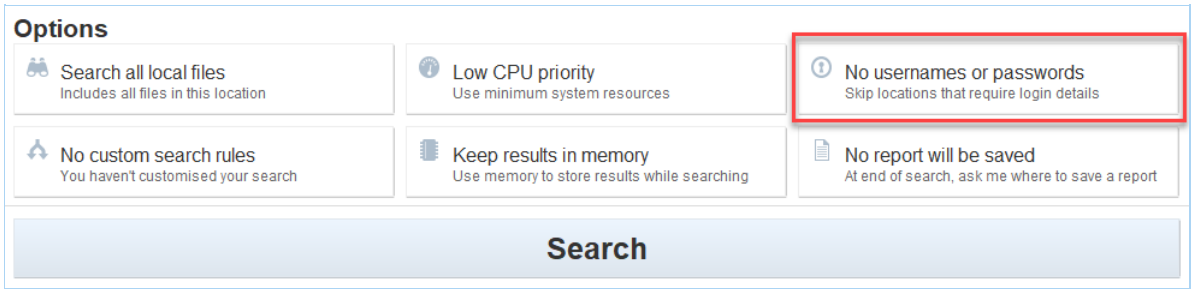
GET AZURE ACCOUNT ACCESS KEYS

1. Log in to your **Azure** account.
2. Go to **All resources** > **[Storage account]**, and under **Settings**, click on **Access keys**.
3. Note down **key1** and **key2** which are your primary and secondary access keys respectively. Use the active access key to connect **ER2** 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 **ER2**.

ADD CREDENTIALS

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



2. In the **Search target credentials** dialog box, click **+ Add** and select one of the following:
   - **Azure Blobs (HTTPS)**
   - **Azure Queues (HTTPS)**
   - **Azure Tables (HTTPS)**
3. 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.
4. (Optional) Under **Encrypt credentials** enter a master password to encrypt stored

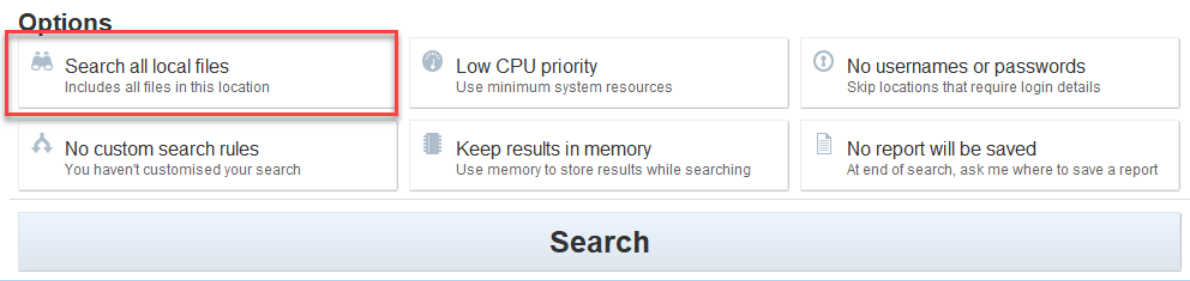
credentials.

> **Tip:** Credentials are only saved if:
> - Search configuration is saved. See Save and Load Options for more information.
> - The results database is saved. See Setting Results Database Options for more information.

5. Click **Ok**.

ADD TARGET

1. In the main menu, click on **Search all local files**.



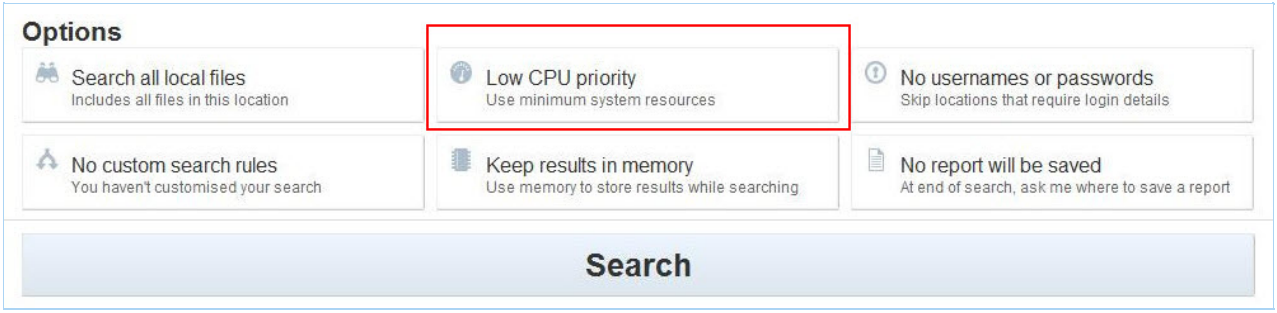
2. In the **Search targets** dialog box, click **+ Add** and select **Cloud Storage**.
3. Select one of the following and click **+** to expand the selection:
   - **Azure Blobs**
   - **Azure Queues**
   - **Azure Tables**
4. In the **Add Azure Storage Account Name** field, enter the Azure Storage account 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 Azure Target.

SETTING RESOURCE USAGE

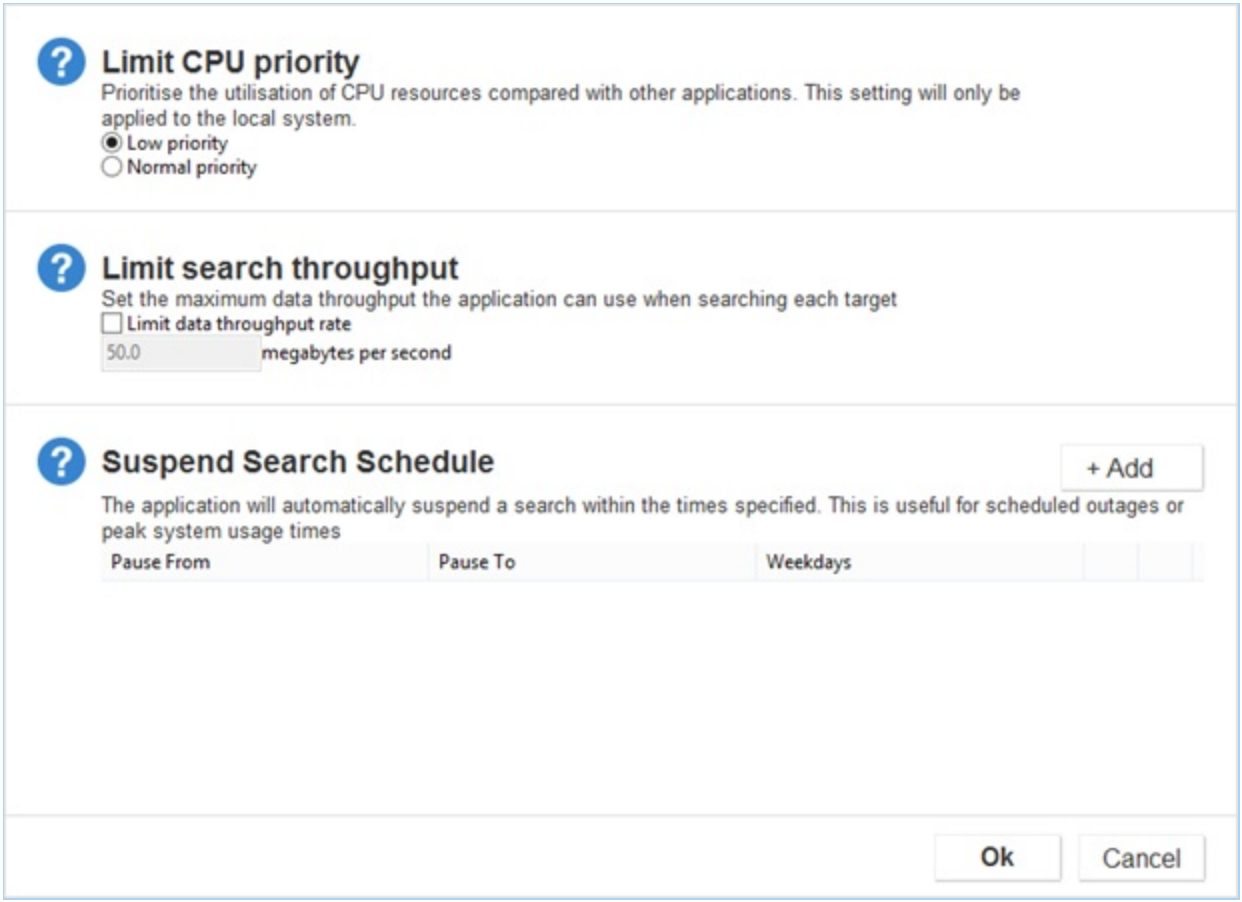
DATA RECON allows you to manage how resource intensive running its scans will be.

Configuring resource usage allows you to manage **DATA RECON**'s impact on system resources, especially on production systems.

To begin setting resource usage for **DATA RECON**, look for the button labeled "Low CPU priority" on the dashboard.



Click on "Low CPU priority" to bring up the resource usage management dialog.



LIMIT CPU THROUGHPUT

DATA RECON will scan TARGETS in "Low priority" mode by default.

This keeps **DATA RECON**'s impact on host systems low so that it can be safely run on production machines.

Selecting "Normal priority" will run **DATA RECON** at a higher CPU priority, which may

cause performance issues on the host system.

> **Info:** Running **DATA RECON** in "Low priority" mode is recommended.

LIMIT SEARCH THROUGHPUT

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

Limiting the rate at which **DATA RECON** scans data will reduce the disk I/O load for the system running **DATA RECON**. If **DATA 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 **DATA 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

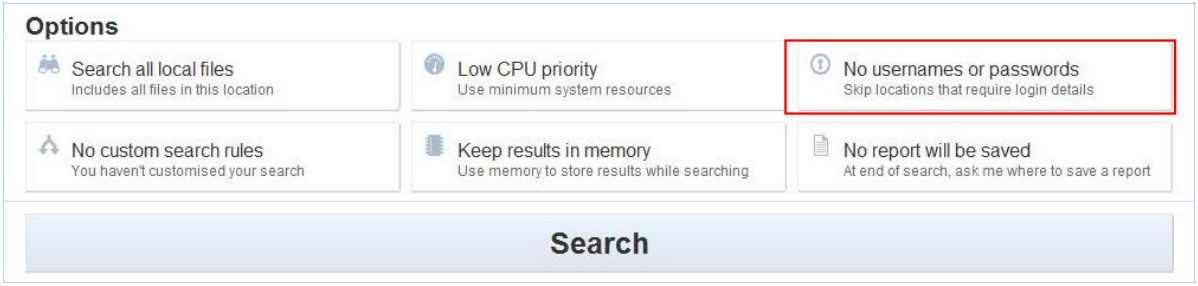
DATA RECON needs valid user credentials before it can scan certain TARGETS.

Note: See Selecting Target Location 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 **DATA RECON** GUI dashboard; clicking it will bring you to the "Search target credentials" dialog.

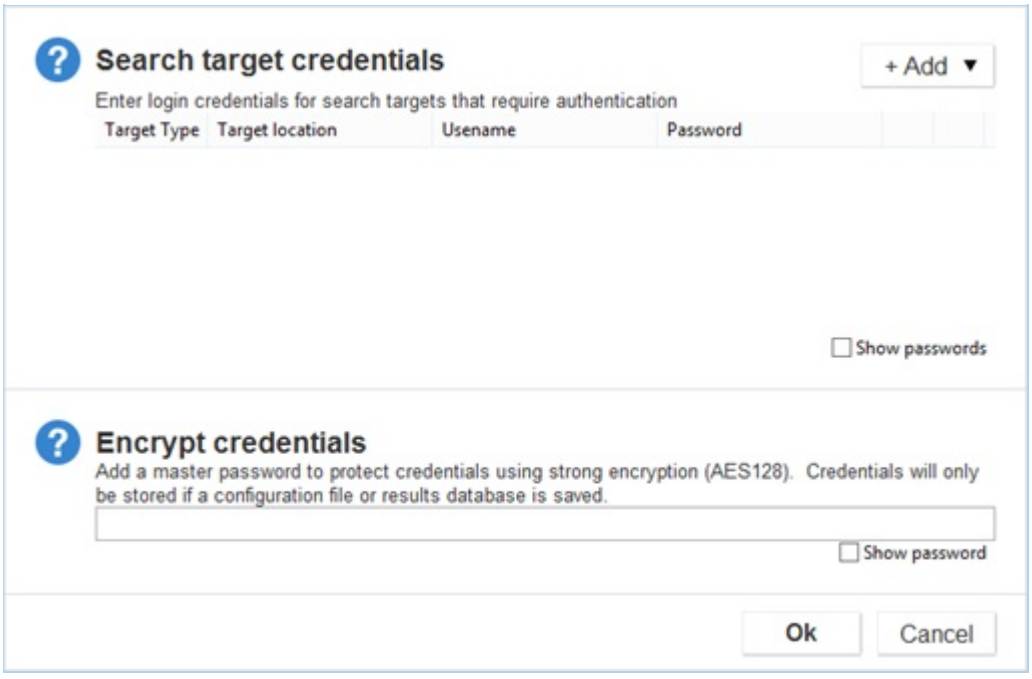


2. Click **+ Add** and select the TARGET type for which you would like to add user credentials for.
3. Fill the fields accordingly.

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.

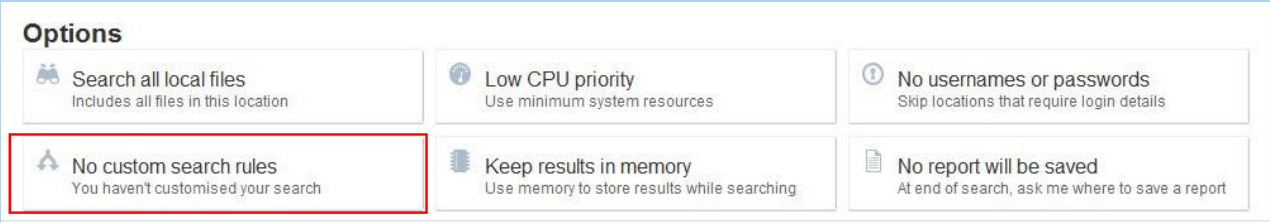
Adding a password here will encrypt the credentials saved in these files.



SETTING CUSTOM SEARCH RULES

You can set up custom search filters to tell **DATA 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 **DATA 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 **DATA RECON** 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. ⚠ **Warning:** 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, `c:\windows\system32` will exclude all files and folders in the `c:\windows\system32` folder, and all the files and folders whose paths start with `c:\windows\system32`.
Exclude location by suffix	Excludes search locations whose paths end with a given string. This is usually used to exclude files that end with a given string. For example, `led.jnl` will exclude all files and folders that end with the string led.jnl from the scan.

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

Search Filter Name	Usage
Ignore match by expression	Ignore matches found during scans if they match a given expression. The syntax of this expression is as follows: • `?` : A wildcard character that matches *exactly one* character; `???` matches 3 characters. If placed at the end of an expression, will also match zero characters. E.g.: `c:\V???` will match `c:\V123` and `c:\V1`, but will not match `c:\V1234`. • `*` : A wildcard character that *matches zero or more* characters in a search string. ◦ `*` will ignore all matches ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`.
Add test data	Report match as test data if it matches a given string exactly. E.g.: Setting this to `4419123456781234` will report matches found during scans that match the given string `4419123456781234` exactly as test data.
Add test data prefix	Reports matches that begin with a given string as test data. E.g.: Setting this to `4419` will report matches found during scans that begin with `4419` as test data.
Add test data expression	Report matches found during scans as test data if they match a given expression. The syntax of this expression is as follows: • `?` : A wildcard character that matches *exactly one* character; `???` matches 3 characters. If placed at the end of an expression, will also match zero characters. E.g.: `c:\V???` will match `c:\V123` and `c:\V1`, but will not match `c:\V1234`. • `*` : A wildcard character that *matches zero or more* characters in a search string. ◦ `*` will ignore all matches ◦ `*123` matches all expressions that end with `123`. ◦ `123*` matches all expressions that begin with `123`.
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.

*Requires **DATA RECON** Advanced Edition

SETTING RESULTS DATABASE OPTIONS

A results database is used by **DATA RECON** to save and track scan progress.

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

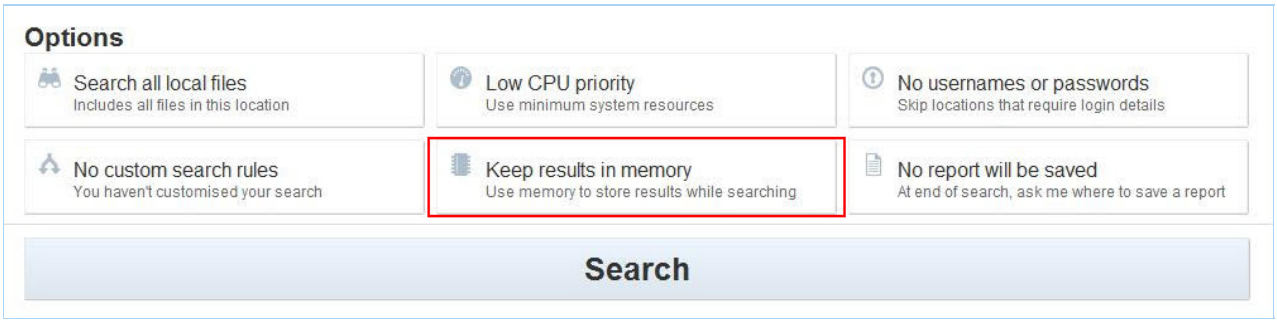
By default, this results database is stored in your system's memory. This means that when you close and re-open **DATA RECON**, your previous results database (and scan/remediation progress) will be lost.

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

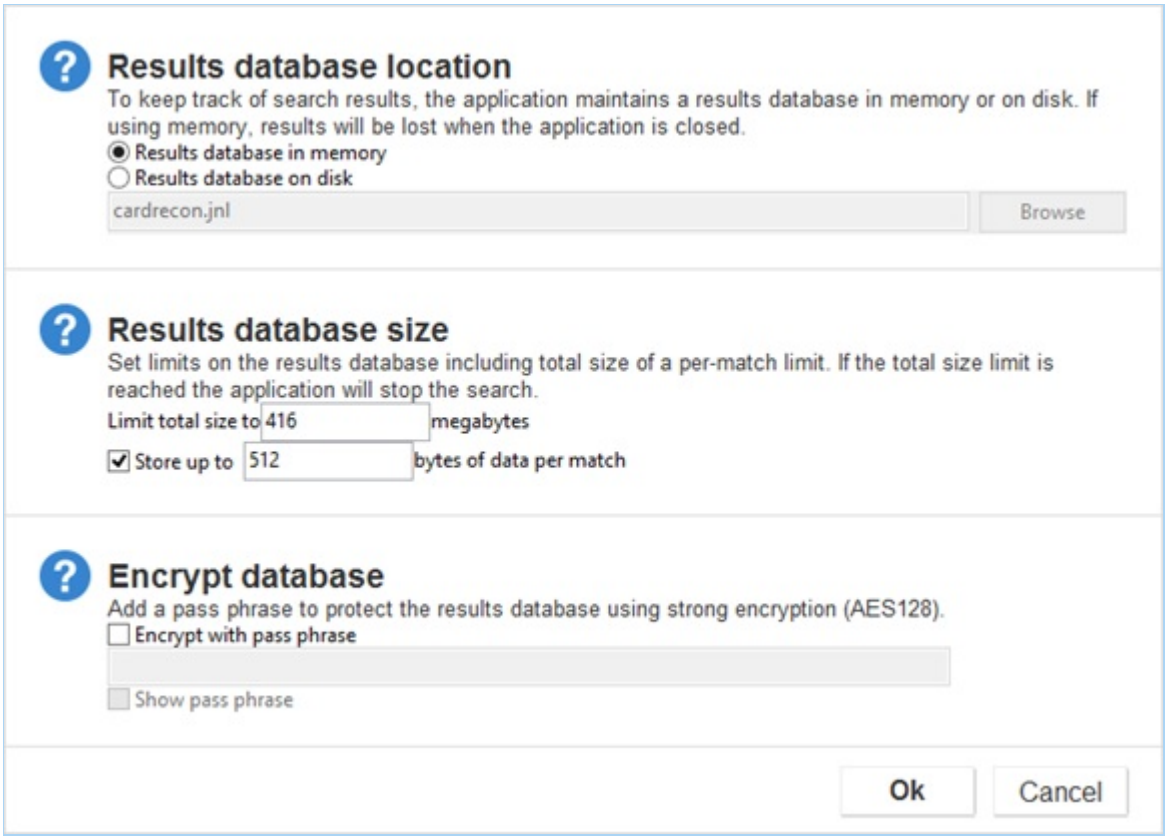
Configuring the how the results database is saved will allow you to:

- Change the default location where **DATA 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 **DATA 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 **DATA 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 `datarecon.jnl` in the "Results database on disk" field will save the results database as `datarecon.jnl` in the same folder as the **DATA 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.

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

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

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

ENCRYPT DATABASE

DATA 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, **DATA RECON** cannot load the database journal file. Please keep your passphrase in a secure location.

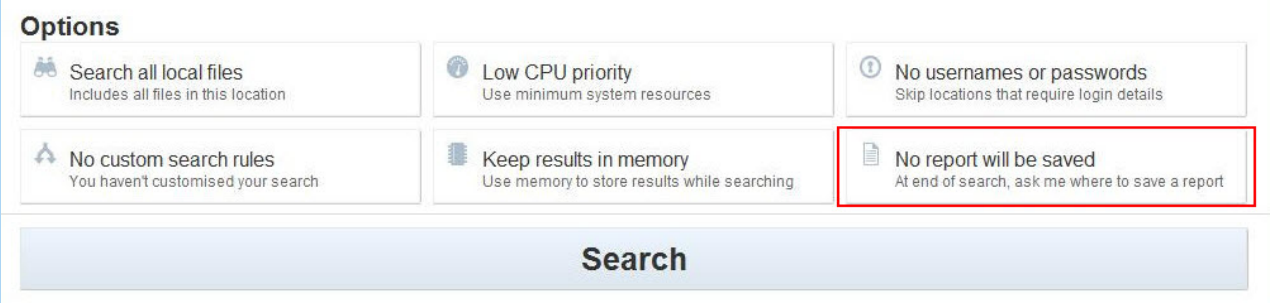
SETTING COMPLIANCE REPORT SAVINGS OPTIONS

By default, compliance reports:

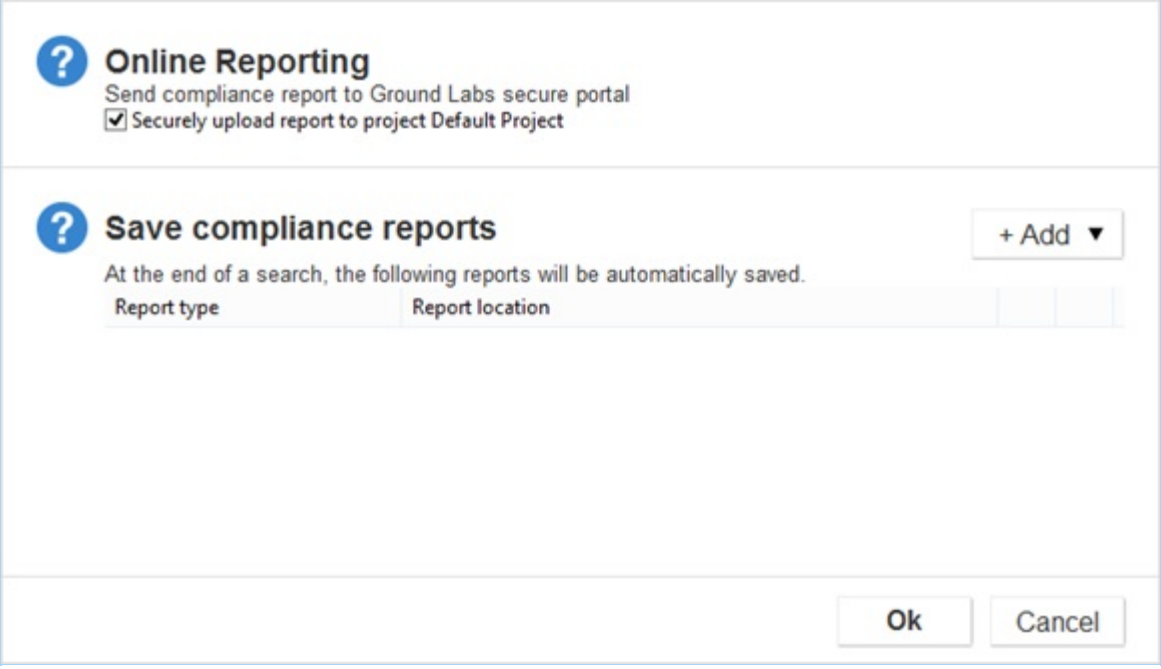
- Will not be saved.
- Will be securely uploaded to the Ground Labs Services Portal.

See Compliance Report for more information.

To configure how **DATA 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, **DATA 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

DATA RECON will prompt you to save a compliance report after each scan.

To configure **DATA RECON** to automatically save a compliance report without prompting you:

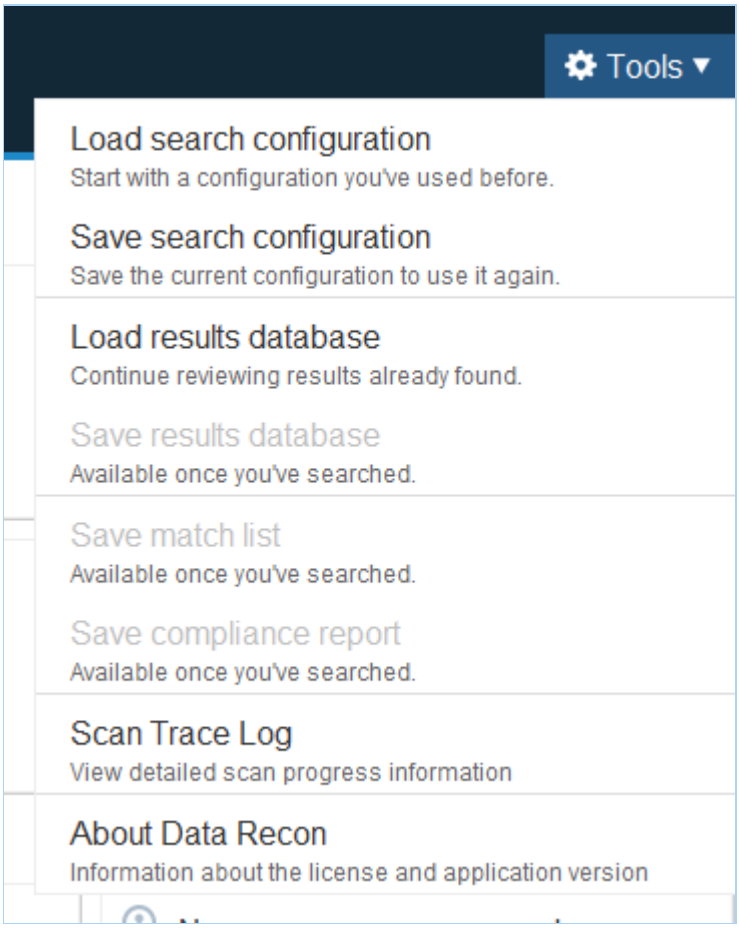
1. Click **+Add** to display a drop-down list of the report formats **DATA RECON** can use.
2. Select your preferred report format from the drop-down list.
3. Type the file path and file name where **DATA RECON** will save the compliance report.

You can save multiple reports in different locations.

Info: DATA RECON will automatically append the appropriate file extension to the file name entered (e.g. `datarecon.pdf` for PDF reports).

SAVE AND LOAD OPTIONS

You can import and save scan options with **DATA RECON** using the "Tools" menu.



SAVING AND LOADING SEARCH CONFIGURATIONS

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

Use the **DATA RECON** GUI to save search configuration files. The **DATA RECON** CLI cannot save search configuration files.

These configuration files may be loaded by both the **DATA RECON** GUI and the **DATA RECON** CLI.

Load Search Configuration

When you click on "Load search configuration", **DATA 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 **DATA RECON** cannot start, your configuration file may be corrupted. Remove the configuration file from the directory **DATA RECON** is placed in and start **DATA RECON**.

Save Search Configuration

Clicking on "Save search configuration" will prompt you to decide where you want to save your current **DATA RECON** search configuration.

SAVING AND LOADING RESULTS DATABASE

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

Load Results Database

When you click on "Load results database", **DATA 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 **DATA 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, **DATA RECON** will allow you to save a list of all the matches found in the current session.

When saving a match list, **DATA 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, **DATA RECON** will ask if you want to save a compliance report if **DATA RECON** is not already configured to save compliance reports.

By default, compliance reports are saved as PDFs.

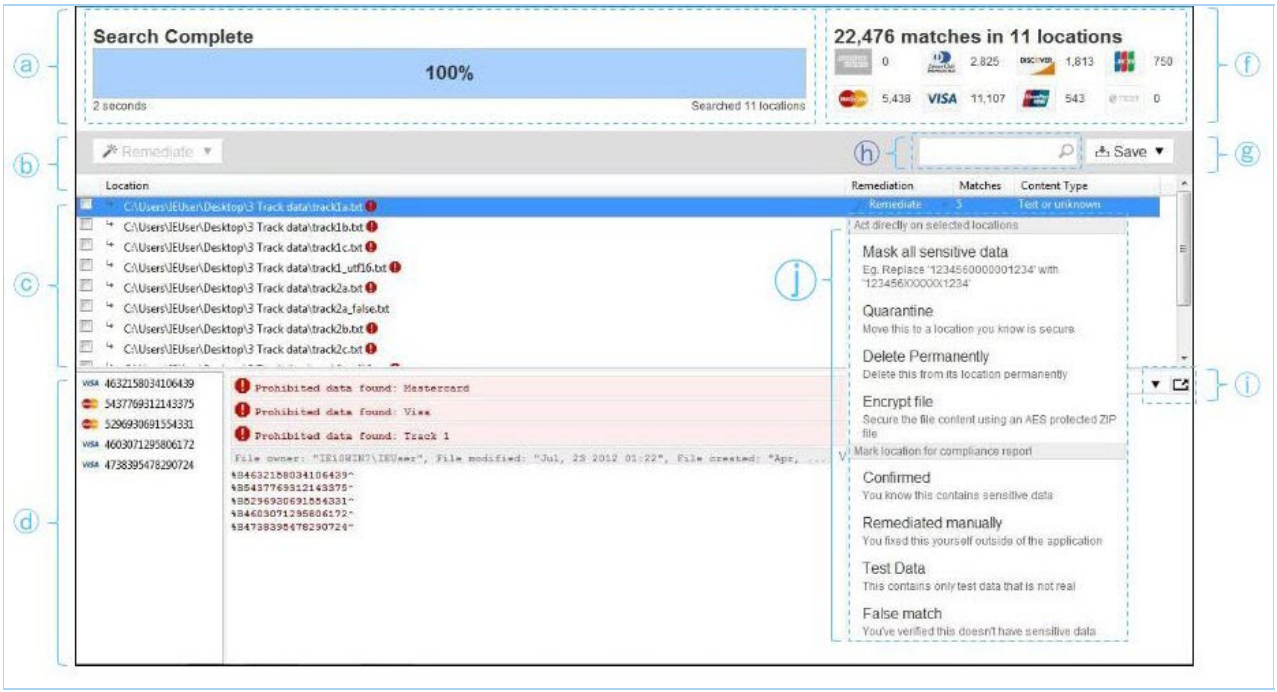
You can save compliance reports as:

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

RESULTS AND REMEDIATION

Beginning a scan on the **DATA RECON** GUI will take you to the **DATA RECON** Results screen.

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



	Label	Description
a	The scan progress bar	Shows the progress of the currently running scan, and controls to stop, pause, or skip files during the current scan.
b	Bulk remediate/mark	Selecting one or more matches in the match list will allow you to remediate or mark matches in bulk. See Remediating and Marking Matches.
c	Match list	Shows list of matched data; selecting an item on this list will bring up its details on the Match Inspector.
d	Match Inspector	Shows specific match details.
f	Match summary	Shows a summary of match data found during the scan.
g	Save results database/match list/compliance report	Save options drop-down menu.
h	Filter matches	Type in search terms to quickly filter match results.
i	Detach Match Inspector/Change Match Inspector view	Clicking on the “detach” icon will detach the Match Inspector from the DATA RECON window; the Match Inspector can display match details as text or as a hex file.

	Label	Description
j	Remediate/Mark matches	For more information on how to remediate/mark matches, see Remediating and Marking Matches.

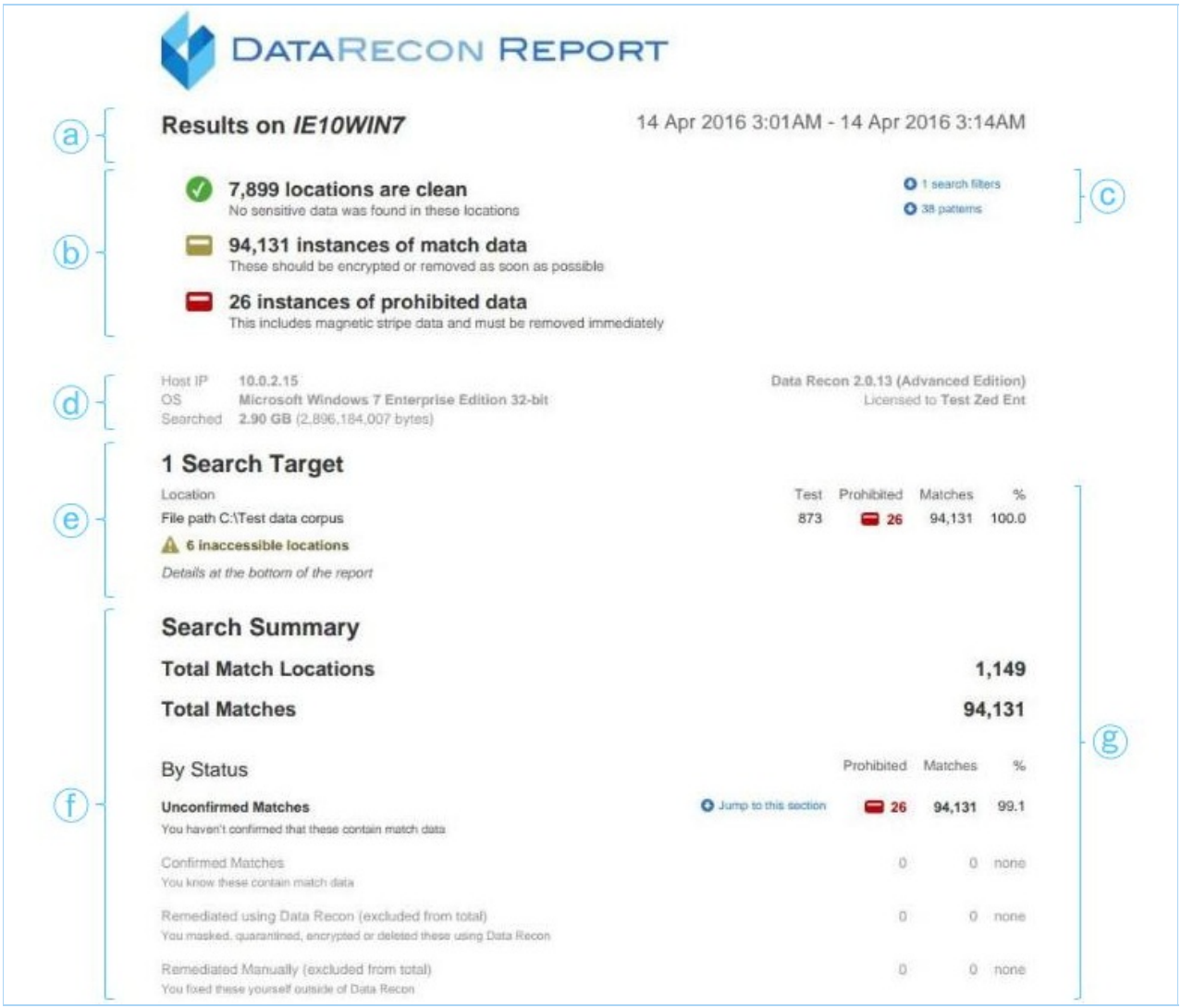
⚠ **Warning:** If you click **Back** to go to the dashboard, and start a new scan by clicking **Search**, you current scan progress will be lost.

Once **DATA RECON** completes a scan, it will ask if you want to save a compliance report.

If you have already configured **DATA RECON** to save a compliance report, **DATA RECON** will not prompt you about report saving.

COMPLIANCE REPORT

The **DATA RECON** compliance report summarizes all of **DATA RECON**'s findings from a given scan.



Label		Description
a	**Date and status of scan**	Gives the host name of the host scanned, the date the scan started, and the date the scan was completed or stopped. If the scan was canceled or stopped (you cannot generate a compliance report unless you complete or stop a scan), the report will state that the scan was "(canceled)".
b	**Compliance summary**	Summary of clean locations, match instances, and locations that contain prohibited matches.
c	**Scan parameters**	Summary of parameters applied to the scan, such as search filters and types of card data.
d	**Host and scan configuration**	Gives the host's IP address, the host's operating system, the total size of the data scanned, the version of **DATA RECON**, and licensee details.

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

"Confirmed" matches are matches that have been reviewed by the user and are found to contain non-compliant data.

- **"Remediated using CARD RECON" ***
  Matches that have been marked as "Remediated using **DATA RECON**" are confirmed matches that have been remediated using **DATA RECON**'s built-in remediation tools.
  Remediating matches with **DATA RECON**'s built-in remediation tools will automatically mark them as "Remediated using **DATA RECON**".
- **"Remediated Manually" ***
  Matches that have been marked as "Remediated Manually" are confirmed matches that have been marked by a user as remediated with tools outside of **DATA RECON**.
  Marking matches as having been "Remediated Manually" will not alter existing data.
  DATA RECON cannot guarantee that matches that have been marked as manually remediated have been effectively remediated to comply with PCI DSS.

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

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

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

- **"Test Data" ***
  Matches that have been marked as "Test Data" are matches that have been reviewed and found to match data that are from test data sets.

  When marking a match as test data **DATA RECON** will ask if you would like to:
  - **"Update configuration to exclude identical matches from future searches"**: This would update **DATA RECON**'s current search filters for the current session, and save a configuration file that contains a custom search filter to exclude the data marked as a false

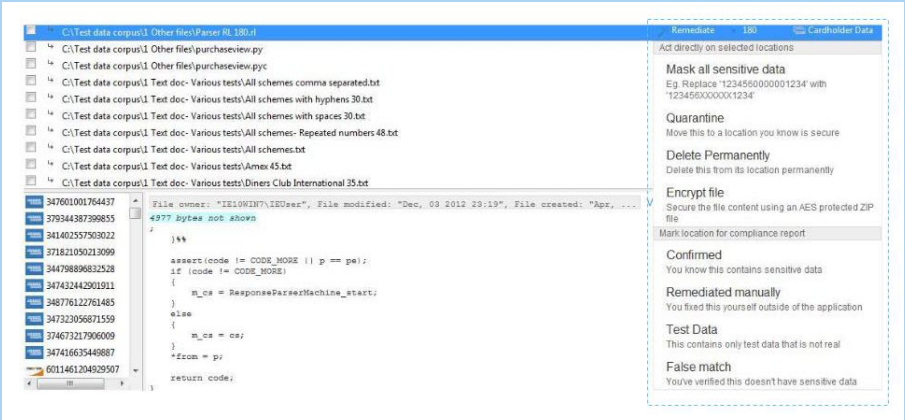
match from future searches. (For more information, see Save and Load Options).

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

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

REMEDIATING AND MARKING MATCHES

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 .



DATA 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 **DATA 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 **DATA RECON**.

DATA RECON COMMAND-LINE INTERFACE

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

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

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

GETTING STARTED WITH THE CLI

Download the appropriate version of the **DATA RECON** CLI from the Ground Labs Services Portal.

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

LOCATE DATA RECON CLI

In the command prompt:

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

In Terminal:

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

RUNNING DATA RECON CLI

In the command prompt:

```
# To run the DATA RECON CLI
datarecon_2.0.xx.exe
```

In Terminal:

```
# Where <datarecon_linux26_2.0.xx> is the file name of the DATA RECON executable
chmod +x datarecon_linux26_2.0.xx
./datarecon_linux26_2.0.xx
```

DATA RECON CLI OPTIONS

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

Command Line Flags	Function
`-o,-output <path>`	Sets the location where the compliance report will be saved. Output formats: • PDF • TXT • CSV • CRR* **Info:** Multiple entries may be used to save several copies of the compliance report in different formats.
`-p, -password`	Encrypt the saved database journal file; **DATA RECON** will prompt you to select a password.
`-password-inline <password>`	Encrypt the saved database journal file; user sets the password in-line, e.g.: `./datarecon_linux26_2.0.13 -j journalfile.jnl -password-inline PASSWORD`
`-q,-quiet`	Runs in 'quiet' mode.
`-r <path>`	Sets the root directory for the search.
`-v, -verbose`	Runs in 'verbose' mode.
`-version`	Displays software version.
`-vv, -very-verbose`	Turn on 'extra verbose' mode. **Tip:** You can save the output from 'verbose' or 'extra verbose' mode for debugging. To do so, you first have to be using an OFFLINE LICENSE FILE. See Offline Licenses. Then, issue the following command: `./datarecon_linux26_2.0.13 -vv >> output.txt`

SETTING UP A WINDOWS VIRTUAL MACHINE

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

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

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

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

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

SYSTEM REQUIREMENTS

To run VirtualBox, your host machine will need:

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

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

DOWNLOAD WINDOWS VM

Microsoft makes its platforms available as VMs for testing purposes here: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

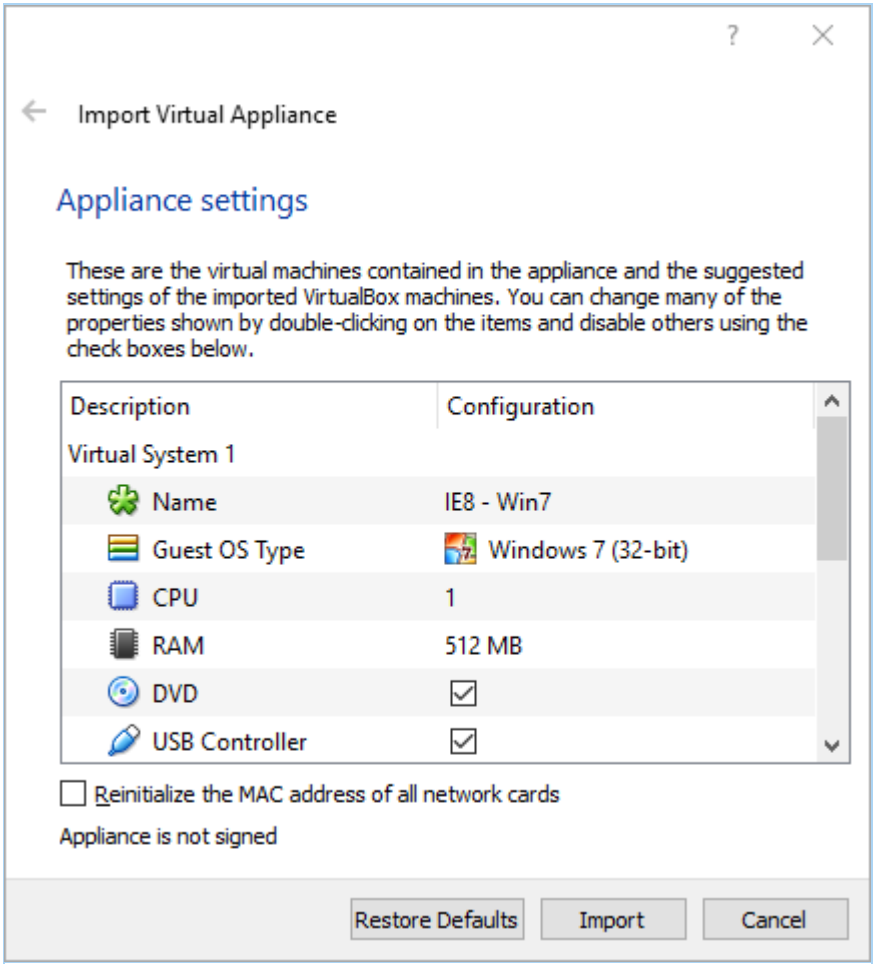
On Microsoft's "Download virtual machines page" :

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

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

INSTALLING THE VIRTUAL MACHINE

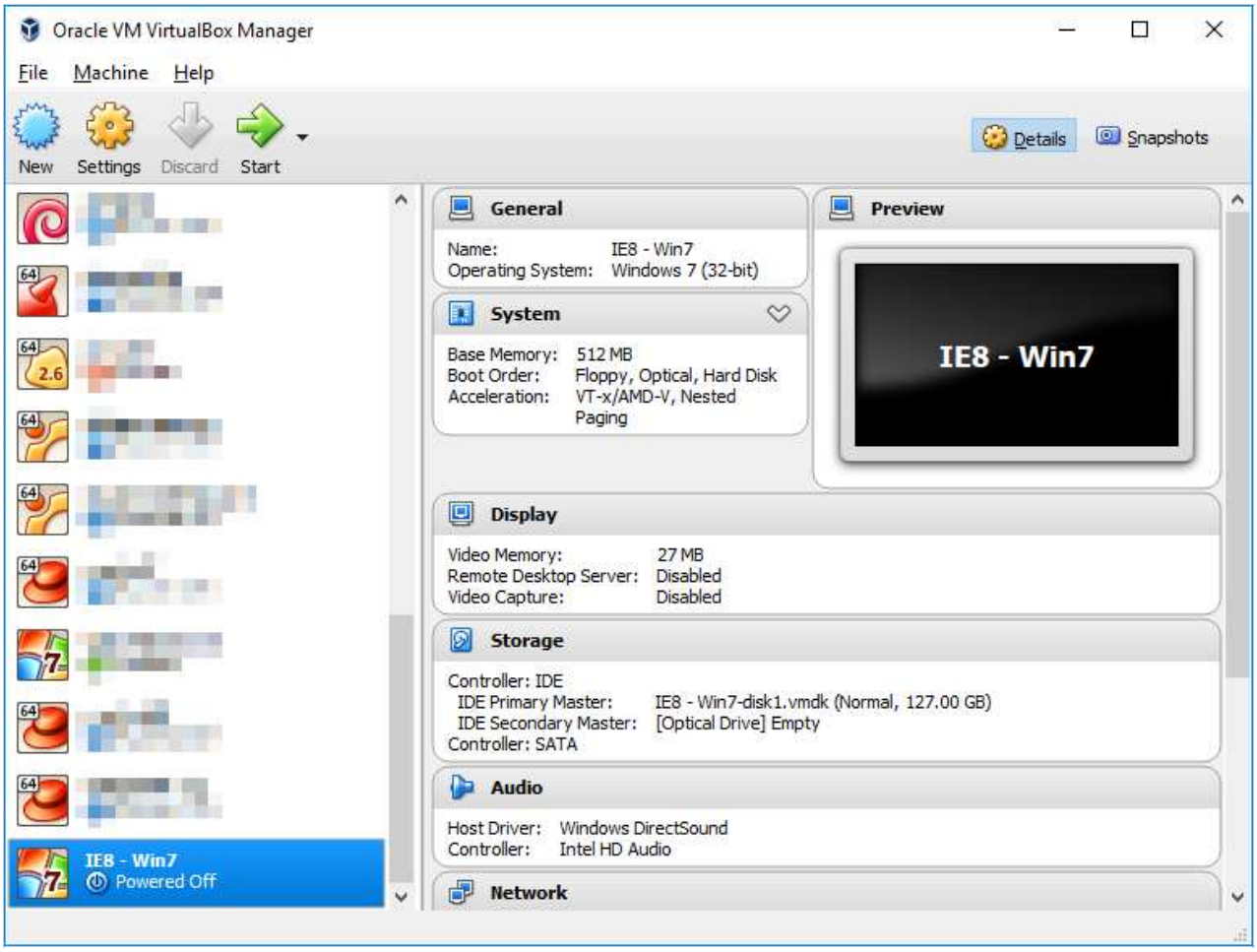
1. Make sure that VirtualBox is installed.
2. Locate the downloaded Windows VM `*.zip` file. Extract the virtual appliance file.
3. Double-click the extracted virtual appliance file (`*.ova`).
   VirtualBox opens and displays the "Import Virtual Appliance" dialog.



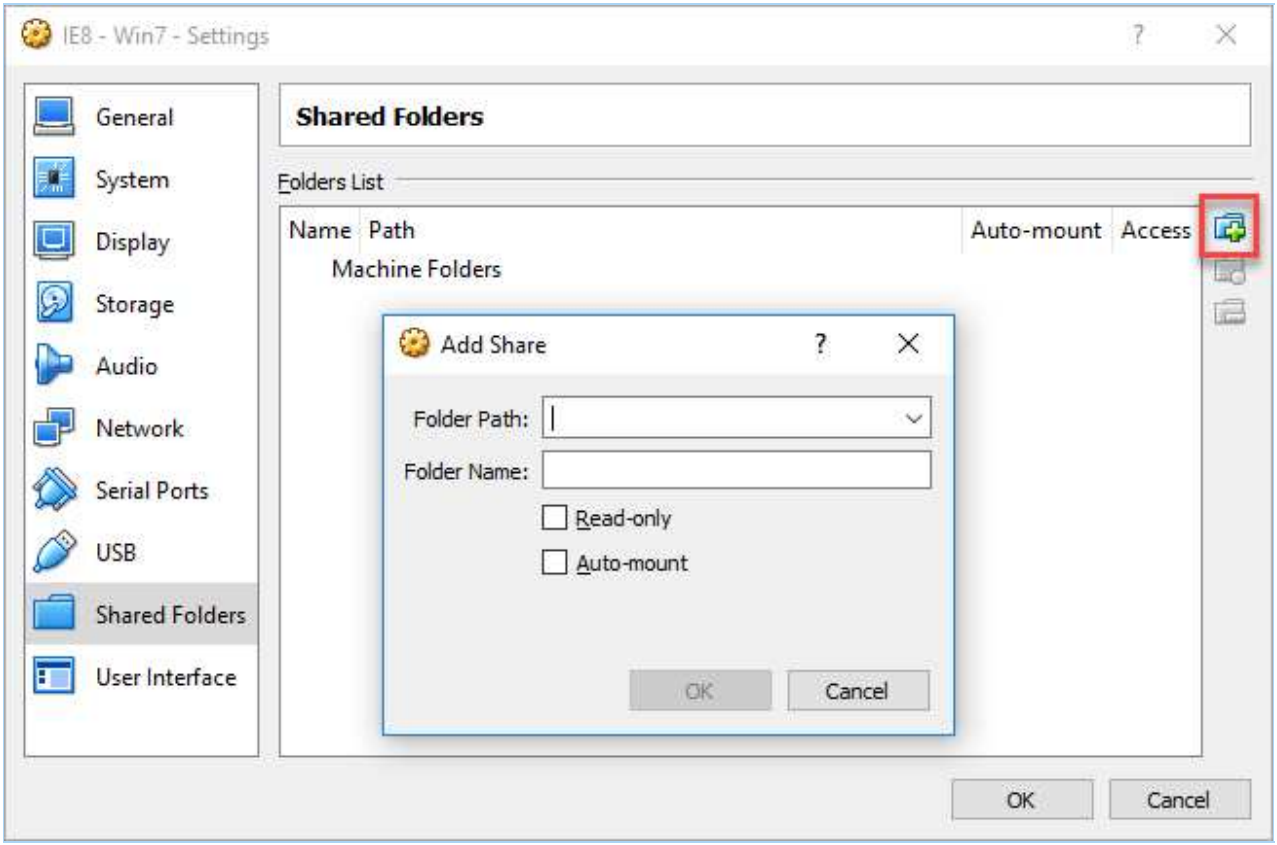
4. Click **Import** to start building the Windows VM.

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

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



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



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

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

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

Download and run the **DATA RECON** GUI on the Windows VM to begin creating and managing your configuration files.

THIRD-PARTY SOFTWARE DISCLAIMER

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

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

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