# USER GUIDE

DARKWEB ID

ID AGENT

16701 Melford Blvd.
Unit 127
Bowie, MD 20715

844-IDAGENT

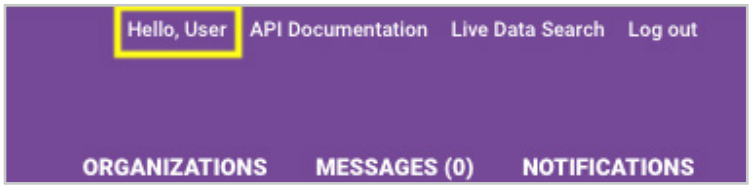


# Table of Contents



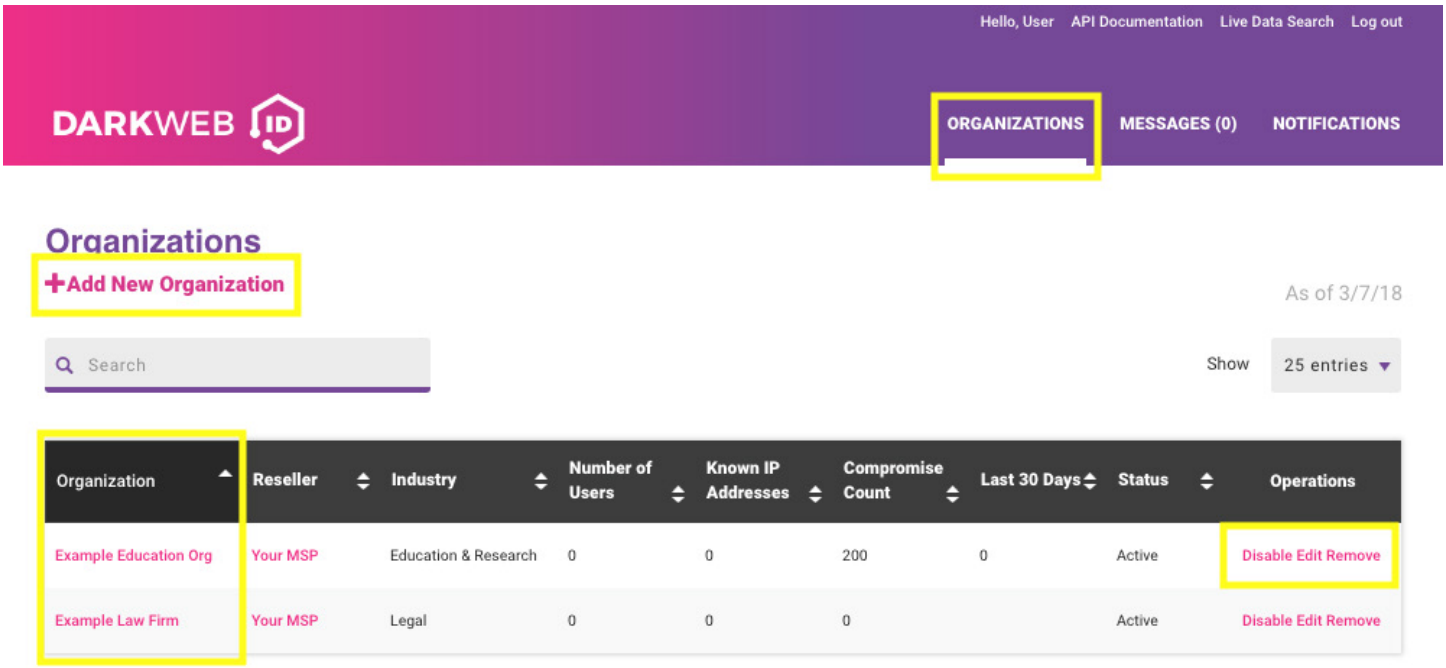
# Account Details

To update account information such as your password, phone number, name, or notification preferences, you can do so by clicking "Hello, your name" in the upper right-hand corner of the Dark Web ID™ platform.



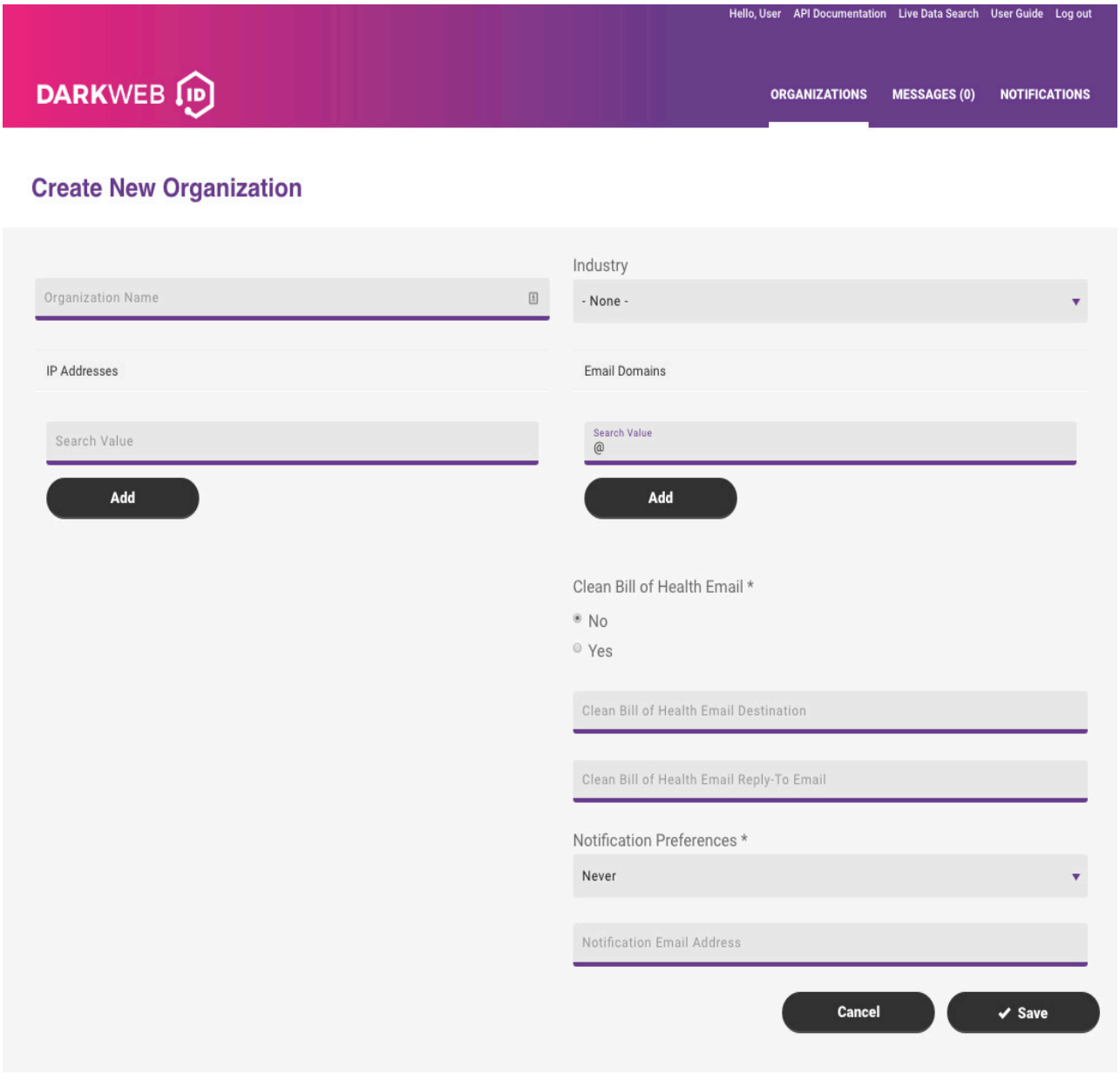

# Organizations

The "Organizations" view will welcome you each time you log onto the platform. Your command center contains a rundown of all your monitored organizations along with administrative options on the right allowing you to "disable, edit, or remove" any organization.




To add new organizations to your platform, click the "Add New Organization" button.

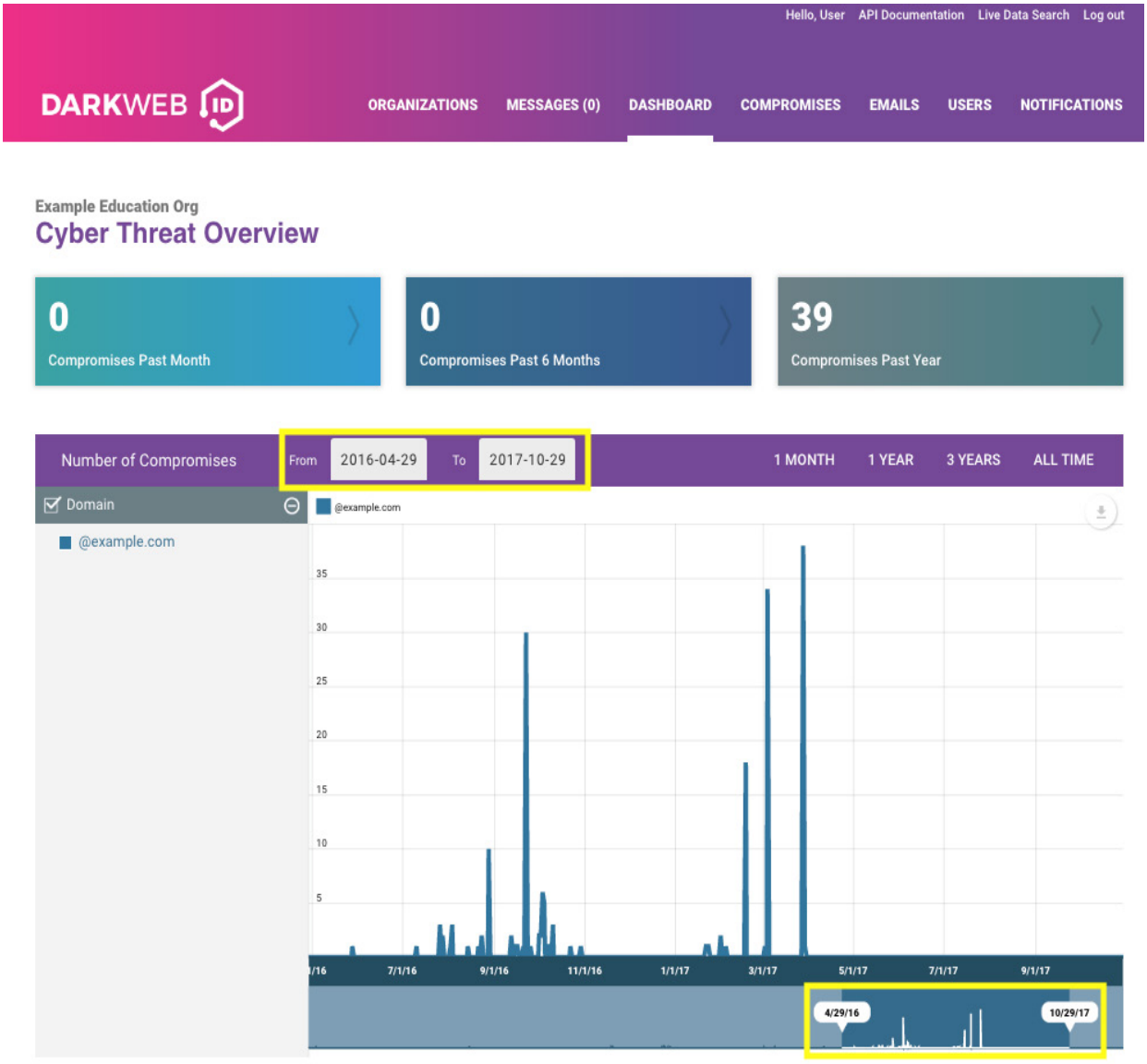
- Organization Name (required) - The name of the organization
- Industry (optional) - The industry of the organization
- IP Addresses (optional at the time of creation) - Multiple IP addresses can be added for monitoring. Click the "Add" button to add the IP address to the organization.
- Email Domain (optional at the time of creation) - Multiple email domains can be added for monitoring. The email domain must begin with an "@" symbol. Click the "Add" button to add the domain.
- Clean Bill of Health (required) - This feature will send an email to the address specified in "Clean Bill of Health Destination" at the end of the month if no new compromises have been added to the organization in the previous month. The destination is likely to be an employee or distribution list of the organization. You are also able to specify a reply-to address for this communication.
- Notification Preferences - An email address can be configured to receive notifications of new compromises. While users have their own notification preferences, this configuration allows you to target any email address. A typical use for this configuration is to send notifications to your internal ticketing system such that tickets can automatically be created when new compromises are detected.




Note: Please allow 24 hours for historical data to completely load into the platform once you have added a new organization. You will receive your first "New Compromises" email after the historical data loads, but please note, the platform sends you this email because it is seeing all the data loading for the first time as new data.

# Dashboard

The "Dashboard" tab or Cyber Threat Overview provides a graphical representation of each organization's compromises. This will be the first screen you encounter once you click into a monitored organization's profile. You can view all the active domains you are monitoring on the left as well as an overview of all the compromises in the past month, 6-months, and past year.



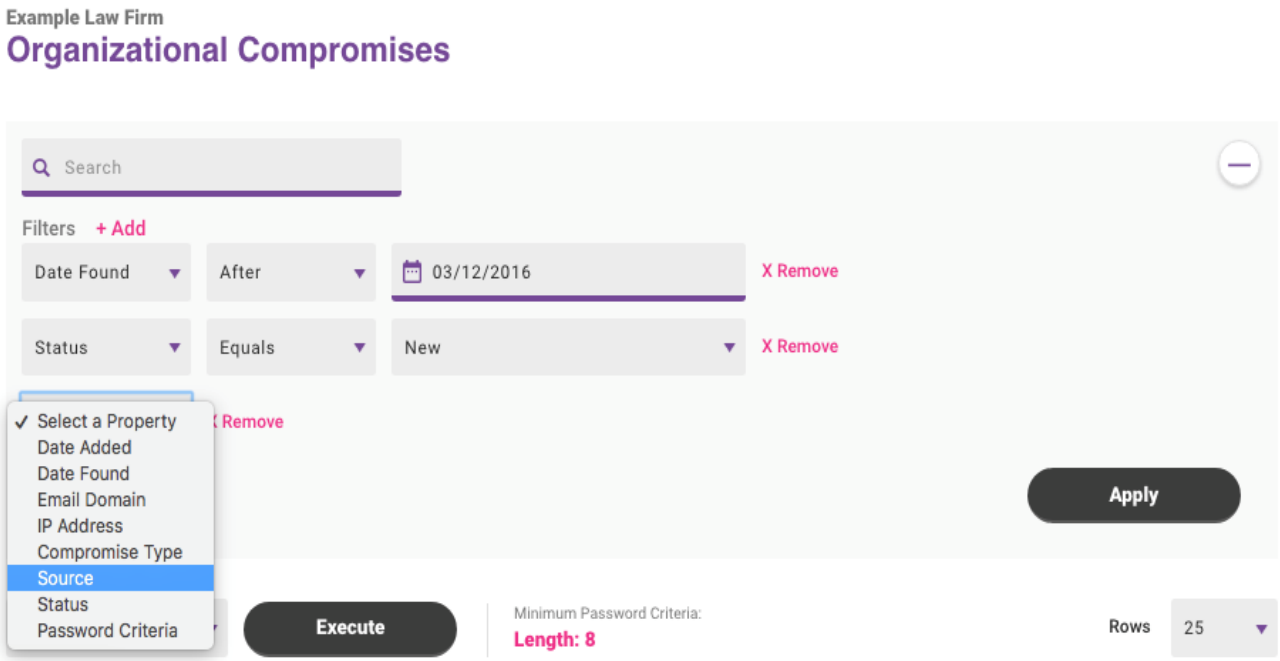

On the bottom of the graph, there are sliders to toggle the date range shown on the graph. The date range can also be selected manually using the date selector or quick filters for 1 Month, 1 Year, 3 Years or All Time.

## Compromises

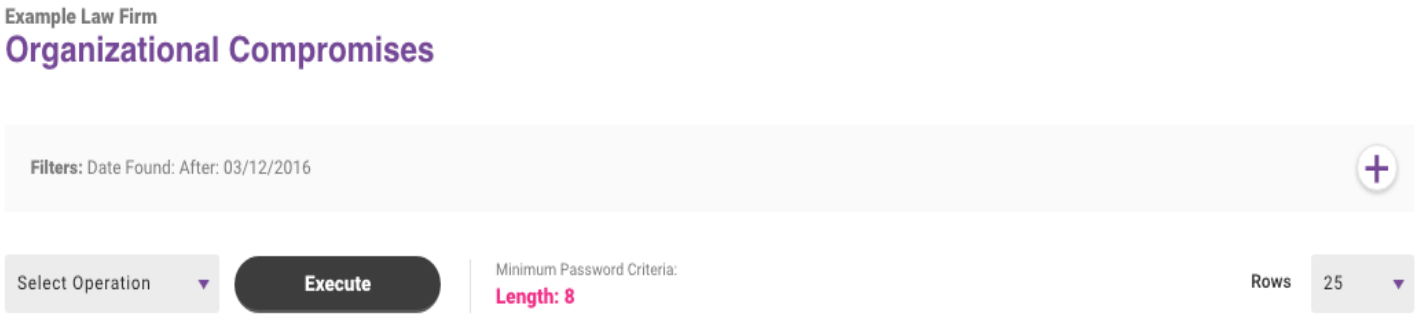
The "Compromises" tab will be your gateway into all the historical compromised credential data for each organization you monitor and all of the domains associated with each. This page gives you the power to navigate and filter through credential information in different ways.

PII (Person Identifiable Information) – When you hover over the "PII Hit" icon, you will see descriptions for other personal information that was leaked along with the Email and/or Password.

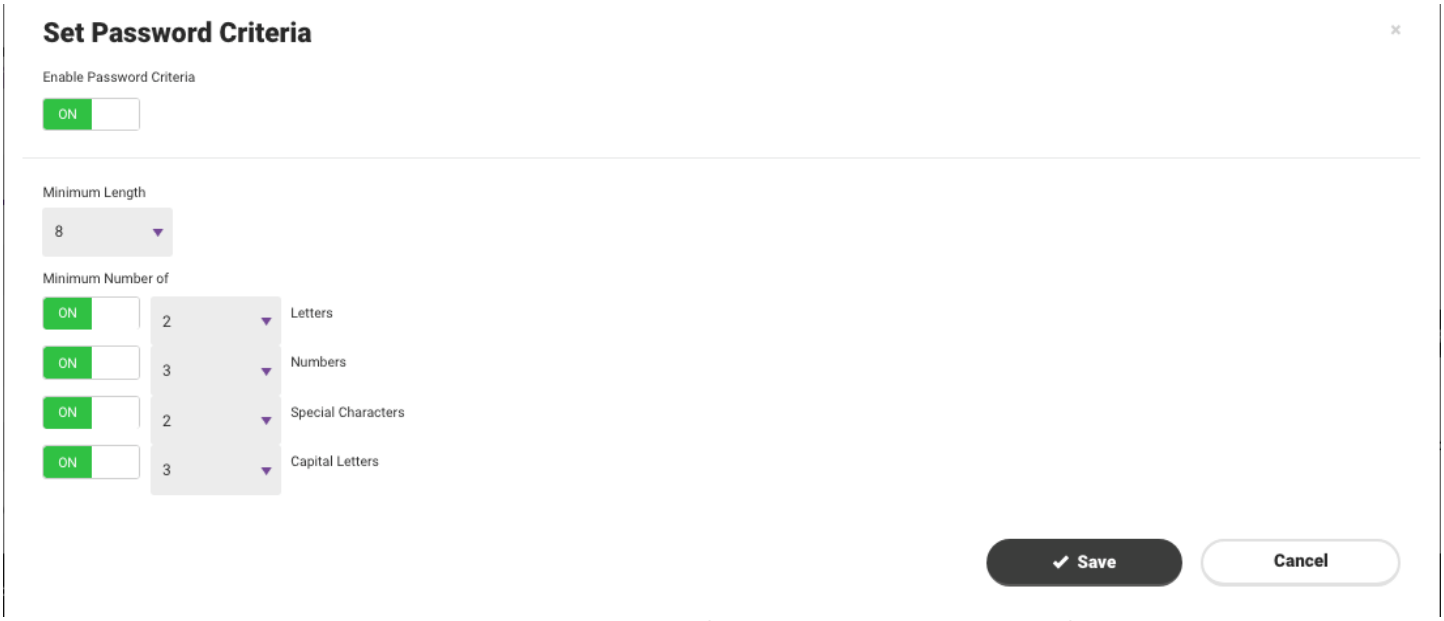
Filters for the compromise list are now constructed by adding criterion to the filter. You'll have access to the same criterion you had in previous versions, but now the filter definition is much clearer and compact. To construct a filter, use the "+ Add" button to define criteria then click the "Apply" button to filter the compromise list. Use the "x Remove" button to remove criterion from the filter and hit "Apply" to update the compromise list.




You can also collapse the filter area to take up less space by using the "-" control in the upper right hand corner. With the filter area collapsed, you'll still be able to see the definition of the active filter. You'll also notice that when Password Criteria are active, the list of active criteria is visible.




The "Set Password Criteria" allows you to enter the specific password boundaries set in place for each client (number of characters, capital letters, etc.). From there, the platform runs a scan against all of the exposed passwords. You will then have a "High" & "Low" status next to the passwords which will meet or come close to the boundaries you have set.



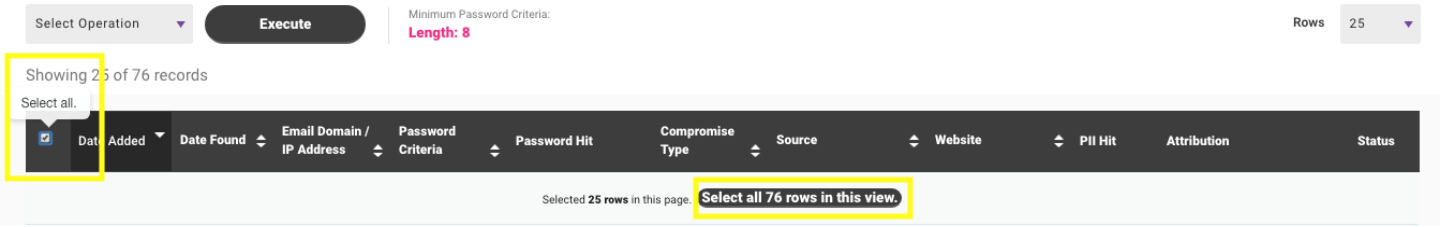

Remember to enable the password criteria at the top of the page, and set as many filters as necessary to match those set by the client's organization. Click "save" and allow the system to recalculate the results.

## Compromise Types/Source

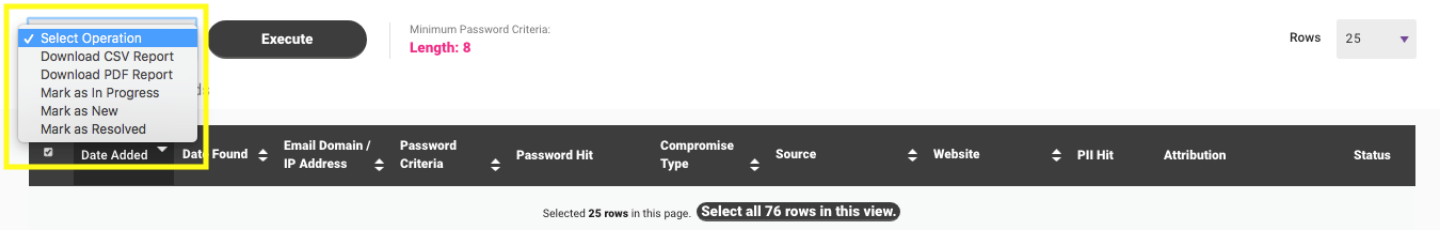
| Compromise Type/Source | Meaning |
|---|---|
| Chat room | Compromised data discovered in a hidden Dark Web internet relay chatroom (IRC). |
| Hacking Site | Compromised data exposed on a hacked website or data dump site. |
| ID Theft Forum | Compromised data published within a hacking forum or community. |
| P2P File Leak | Compromised data leaked from a peer-to-peer file sharing program or network. |
| Social Media | Compromised data posted on a social media platform. |
| C2 Server/ Malware | Compromised data harvested through botnets or on a command and control server. |
| Tested | The compromised data was tested to determine if it is live/active. |
| Sample | The compromised data was posted to prove its validity. |
| Keylogged/Phished | The compromised data was entered into fictitious website or extracted through software designed to steal personally identifiable information (PII). |
| Breach | The compromised data was exposed as part of a company's internal data breach or on a 3rd party website. |
| Accidental Exposure | The compromised data was accidentally shared on a web, social media, or peer-to-peer site. |
| Malicious / Doxed | The compromised data was intentionally broadcast to expose personally identifiable information. |

## Downloading a Report

All the filtering tools within the "Compromises" tab are useful when it comes time to download a report.




Selections do not carry over from page to page. If you wish to select more options than a single page view allows, use the select all checkbox that appears after selecting the universal checkbox in the purple row.




A compromise report can be downloaded in both a CSV and PDF file from the "Compromises" tab. Selecting the checkbox to the left of the compromise indicates that the compromise will be included on the report after selecting from the "Choose an operation" dropdown.

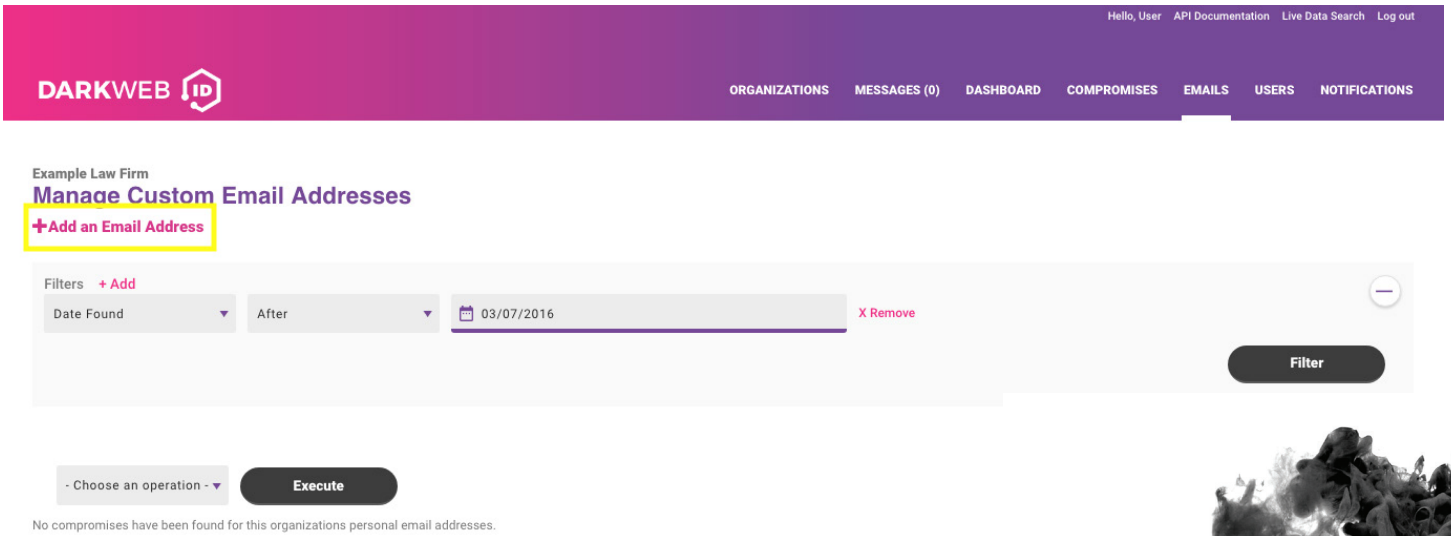
The CSV Report will download an excel spreadsheet with all the data in one document.

The PDF Report will download a clean and finished report showing 25 compromises per page.

Utilize the filtering tools to ensure that only records of interest are included in your download. Additionally, more compromises can be shown per page by changing the "show" option from the dropdown menu.

# Emails

Dark Web ID™ gives you the ability to offer an unmatched level of security. Along with the ability to monitor an organization's domain, you can offer corporate level employees the option to have their personal email accounts (gmail/yahoo/hotmail) monitored for any possible exposures on the dark web

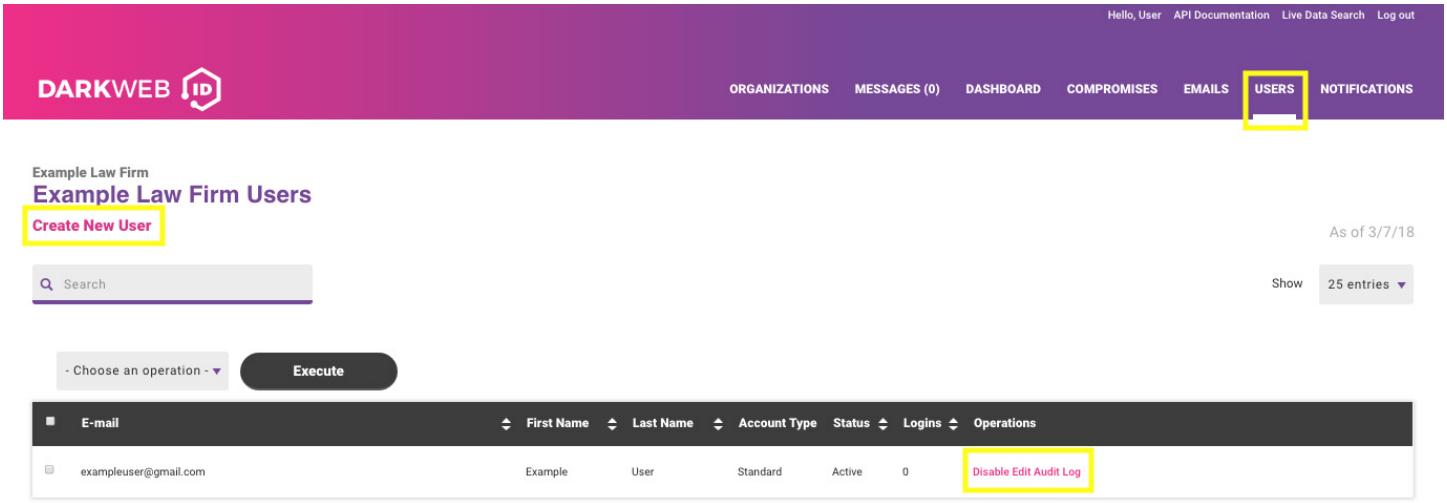



To add an email, click "add an email address" button and input the full email address when you arrive at the next screen and hit "submit". If any of the email addresses' you add have compromises, they will show up on the bottom along with the compromise type, source, and website.

To filter results through different monitored email addresses, click the "Email Address" drop down and select between the different email addresses you've added.

# Client Users

From the "Users" screen, you can manage all your 3rd party client users with access to their organization's portal. From here, you add a client (CEO or IT Manager) with access to ONLY their organizations compromises as well as permission to receive personalized emails when new emails/ passwords are found on the dark web. This page allows you to add a new client user, edit their permissions, suspend access to their account or track their activity.




**Disabling** a user keeps the user's account information in the Dark Web ID™ application, but restricts the user's access and will not allow them to login. Disabled users will still receive Compromise Record Alert emails.

**Enabling** a user will allowed a disabled user to access the site again.

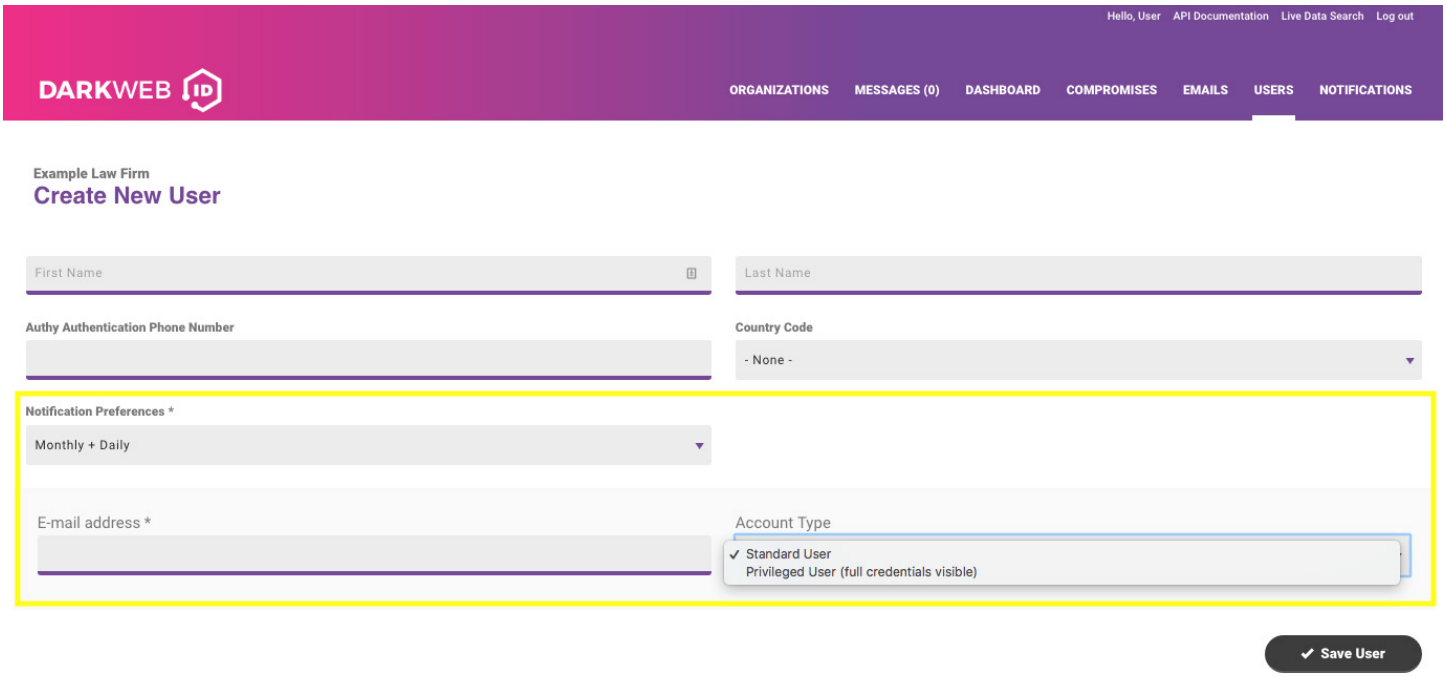
**Audit Log** will give you a summary of how many times a user accessed the platform and when they accessed it.

# Adding a User

After you input the user's email address - There are 2 types of user accounts that can be selected from the "Add a user" screen;

**Privileged User** – A privileged user is created by any global admin, once an organization is created. This account type has the ability to view all exposed emails/passwords, download any compromised credential report, and view the user list for their organization.

**Standard User** - A standard user is created by a Global Admin, once an organization is created. Standard users have the same access as priviledged users, except they cannot view passwords and they cannot view the user list for their organization.

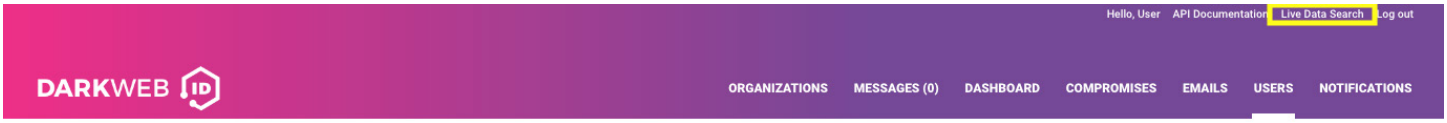



The notification preferences are where you can set your client up to receive the "New Compromise" emails for when emails/passwords are found on the dark web.

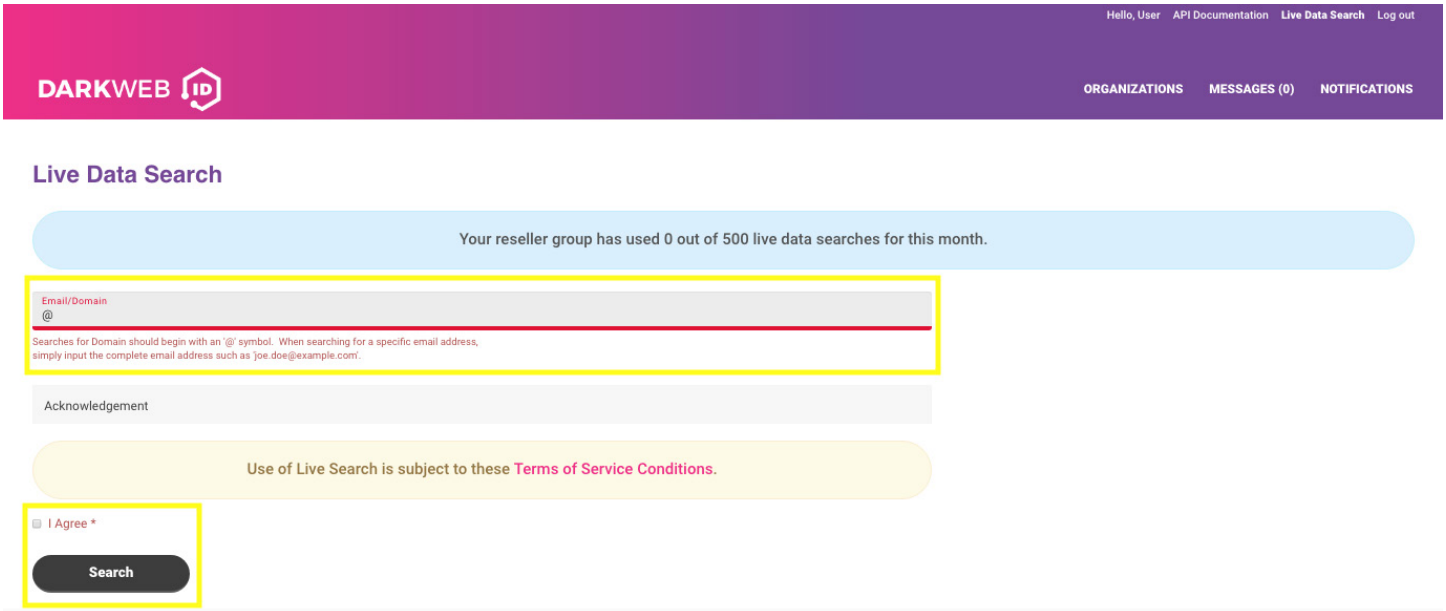
Your client user's will receive an auto-generated email from the platform asking them to log in and finish setting up their account. They will be restricted to only the data associated with the organization you set them up in. They will not have access to your personal list of monitored organizations or the "Live Data Search" function.

## Using the Live Feed

The Live Search tool produces a sample data set of the 100 most recent records in the past 24 months. In accordance with current privacy laws, the data available within the live search will only show the first 4 characters of the exposed password (Ex. Pass********). The full password will be available after you begin tracking a domain under the Organizations tab.

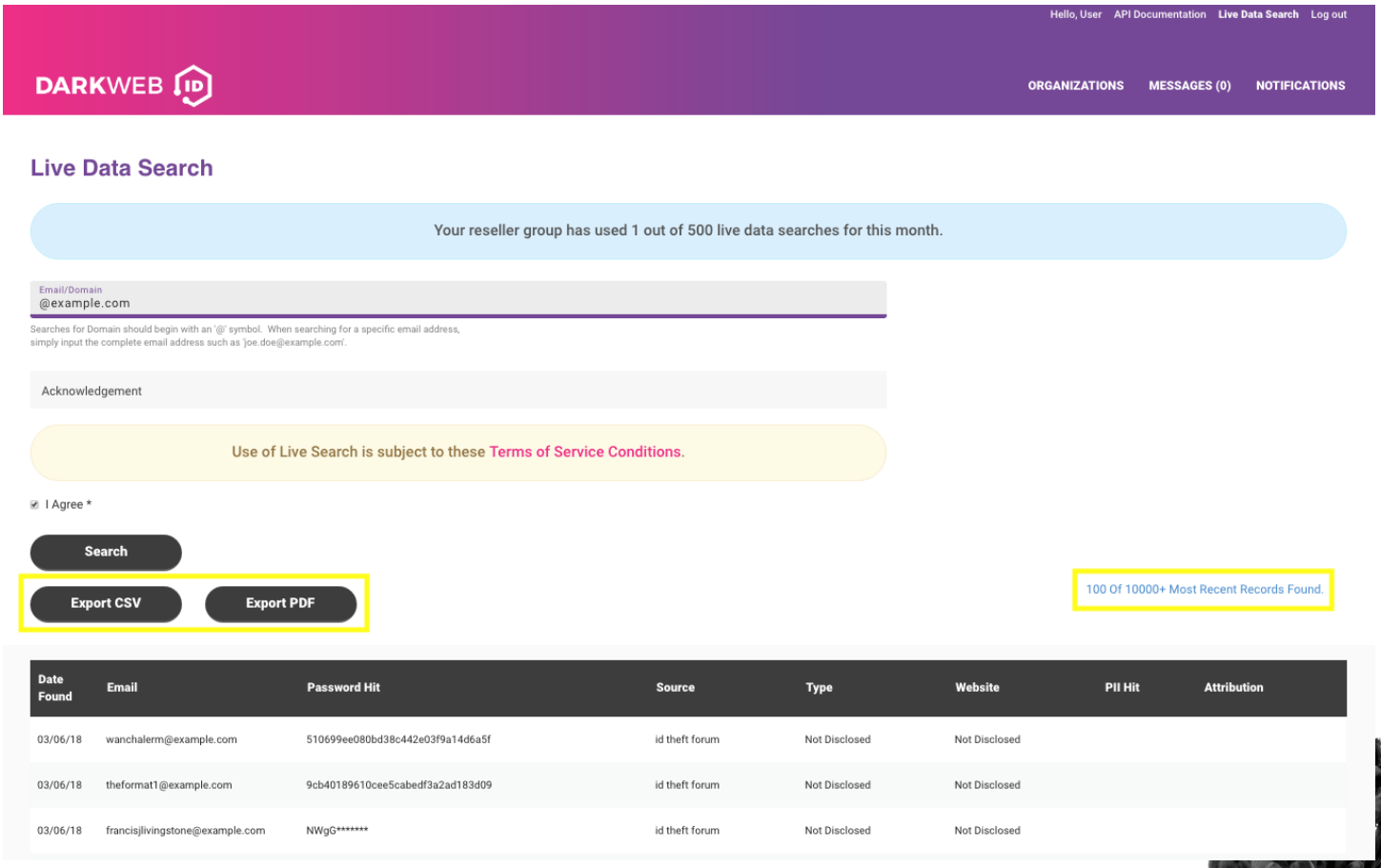



After clicking "Live Data Search" enter the domain under "Email/Domain". Example: @Bestbuy.com (Note: each domain must include "@" for the search to work correctly.) Make sure to check off the "I Agree" checkbox before hitting "Search" for the results to load.




After hitting the "search" button, results for the 100 most recent compromises in the last year should appear along with the total amount of compromises associated with that domain. All the data is also exportable through the "Export CSV" and "Export PDF" button.

The results will list as much attribution as we can provide along with the PII which will show you any extra personal information that was leaked onto the dark web along with any emails and passwords.



The “Password Hit” field will have asterisks following the first 4 characters of the password. For example – Computer123 will show up as Comp*******. The remaining characters of the password will show as clear texts when you set up the domain within the “Organization” feature in the platform.

Note: The “100 of 10000+ Most Recent Records Found” will represent the total count in the past 24 months. The total number of historical compromises may or may not be higher after loading an organization into the domain monitoring feature of the platform.

**Have questions?**

**Contact your Dark Web ID Support Team**

**support@darkwebid.com**