UFED Cloud

Using an account package

1. Using an account package

UFED Cloud assists law enforcement agencies and enterprises to enhance their investigations with information from cloud-based data sources.

Cloud data sources refers to services provided to consumers over the Internet i.e., Dropbox, Facebook, Twitter, Gmail, Google Drive, Kik, Google Contacts, Google Search History, IMAP, Instagram, and VK etc. This solution reduces the time required to solve additional cases.

An account package is a *.ucae or .ucaepc file exported from Physical Analyzer. It contains saved account tokens, cookies, or user credentials which can be used in UFED Cloud to authenticate accounts with minimal traces.

When using an account package, there are two methods based on where your UFED Cloud is installed:

» **UFED Cloud is installed on a separate machine:**
   » The first step is to export an account package from Physical Analyzer or from another extraction tool, such as the Cloud Login Collector.
   » The next step is to import the account package into UFED Cloud. UFED Cloud will then display the available accounts and the user can then select which accounts to authenticate.
» **UFED Cloud is installed on same machine as Physical Analyzer:**
   » The cloud extraction is executed and displayed in Physical Analyzer without the need for an import.

## Importing an account package into UFED Cloud

1. In the menu, click **Cloud > Extraction > Private cloud data**. The following window appears.

> Mandatory fields are indicated with a red border.

2. Enter the new person's first and last name.
3. Enter the Case number, Examiner name, and Examiner ID.
4. Select the options you wish to run on the case (e.g. Media classification, Time zone, Create report, etc.).
5. Click **Next**. The Data sources window appears:

Cellebrite

6. Click ⬇ Import account package to import a *.ucae or .ucaepc file, that has been exported from Physical Analyzer.

7. The following window appears the first time an account package is used:
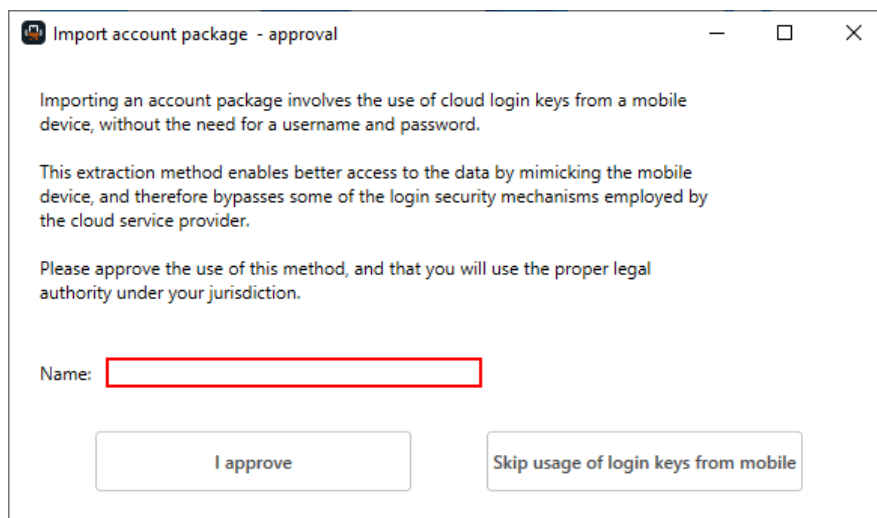
> 📄 This window provides an indication that an account package includes the use of cloud login keys from a mobile device and must include proper legal authority under your jurisdiction.

8. Enter your full name, and click **I approve.**
9. Select the account package file and click **Open**.
10. The account package opens in a new tab.
11. Select data sources from account package.
12. Click **Next**.
13. Follow the steps in the wizard to complete the extraction process.

Exporting an account package from Physical Analyzer

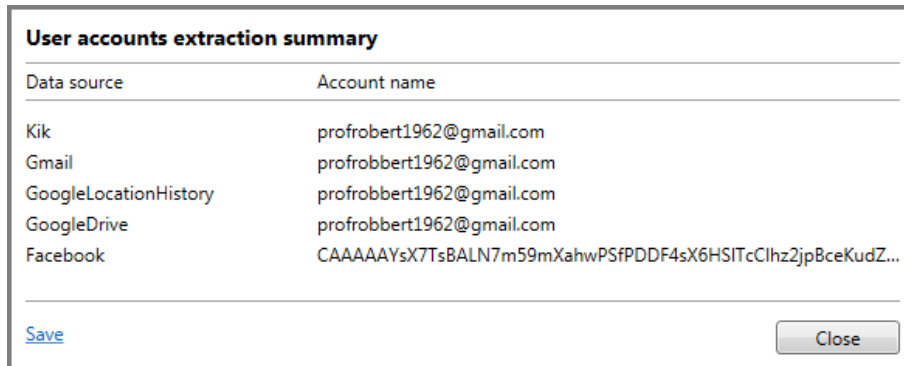Export an account package to extract cloud accounts using tokens.

> 📄 This step is only necessary if UFED Cloud is installed a separate machine than Physical Analyzer.

1. Open an extraction in Physical Analyzer.
2. Select **Tools** > **Export account package**.
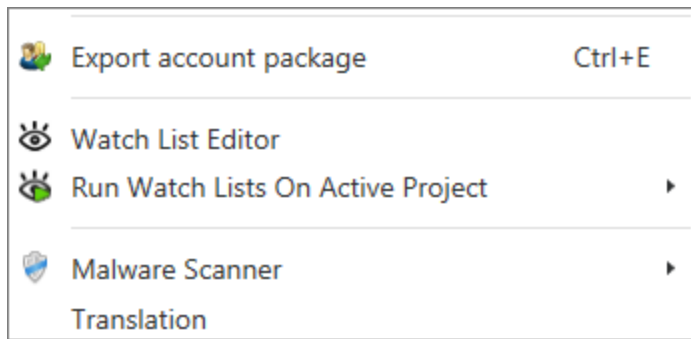
The Save As window appears.

3. Click **Save** to save the Export file (*.ucae) file. The following window appears.

4. Click **Save** to save a text file summary of the extracted user accounts, or click **Close** to complete the process. (The summary may be useful when preparing search warrants, or to share with other investigators.)

> Multiple entries for the same data source may relate to different accounts that were used on the device, or to previous login information for the same account.

Cellebrite