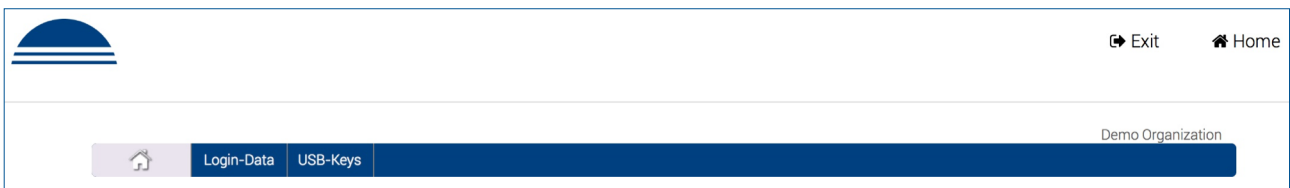# Enterprise Services

**Phrase-Lock Enterprise Services** offer a very simple way to edit, distribute and synchronize login data. Private individuals can easily create and manage login data online for their USB-Key. Professional users have an advanced license to manage any number of USB-Keys.

Please read these instructions carefully - it's all about your data! Some details appear somewhat technical, but we are committed to transparent presentation in order to convey to the user that we are able to deal with secrets - your login data - while not having to know the secrets in terms of content.

*Please note: Phrase-Lock Enterprise services overlap partially with the backup and recovery functions. However, they are not a replacement for current backups.*
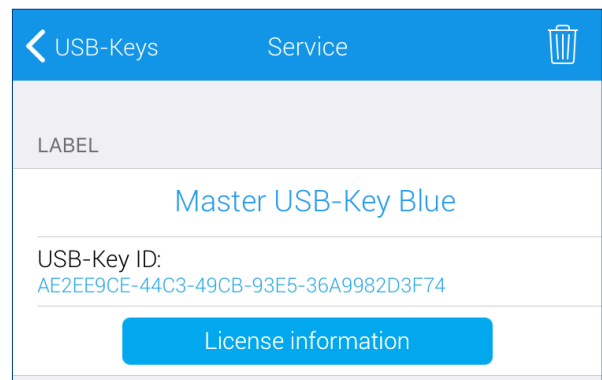
## Activation of the Enterprise Services

The Enterprise-Services must be activated first with a license request. Then a synchronization key with PIN code, hereinafter referred as the S-Key, must be created. This S-Key is necessary to make login data available to other USB-Keys resp. their users.

The S-Key is used to secure and lock the login data for transportation. Like in a transport box with a lock. Only those persons who also know the PIN code are able to receive and read in the login data. On a technical level, this is much more complex and safer than the simple analogy of a transport box. However, a detailed description of the entire encryption process goes beyond the scope of this manual.
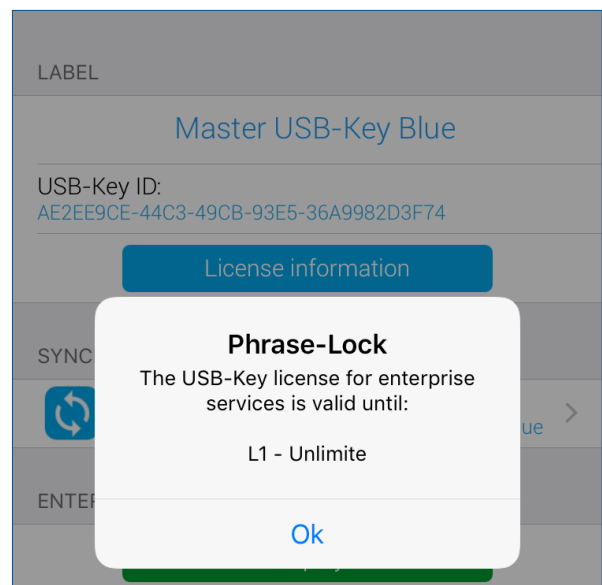
*Please note: This manual requires that a USB-Key is installed on a cell phone and a master-key has been applied in order to use the backup and restore functions, for example. It is also assumed that the user can create and edit login data on his cell phone or he has already done so.*

In the first step, tap **Settings - USB-Key Organisation** - *Selection of the desired USB-Key*.
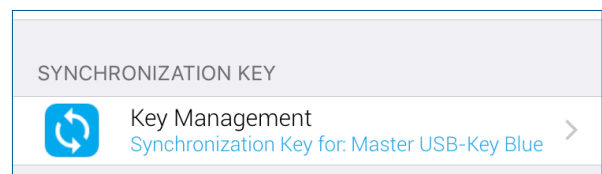
Now press the blue button **Licence information**.

If the previously selected USB key has an appropriate license for enterprise services, the license with validity period is displayed in this message window.
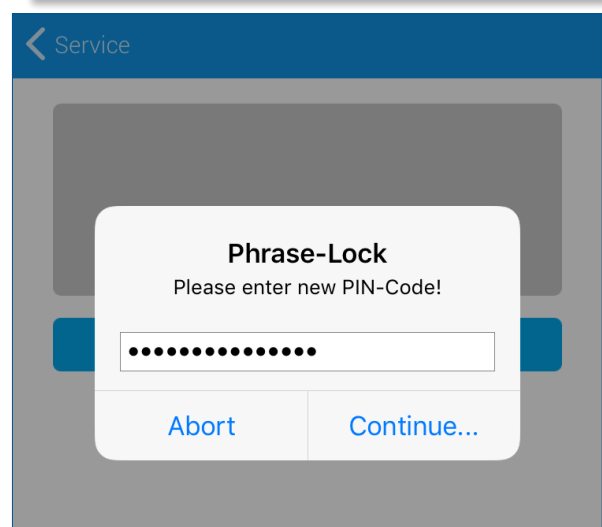
Please now confirm the message window and press the new menu item **Key Management**.

Tap on **Initiate Key** and enter a PIN-Code. The PIN-Code should have a length between 4 and 12 characters.

Press **Continue** and please note the message window! Read the note and follow the next step.
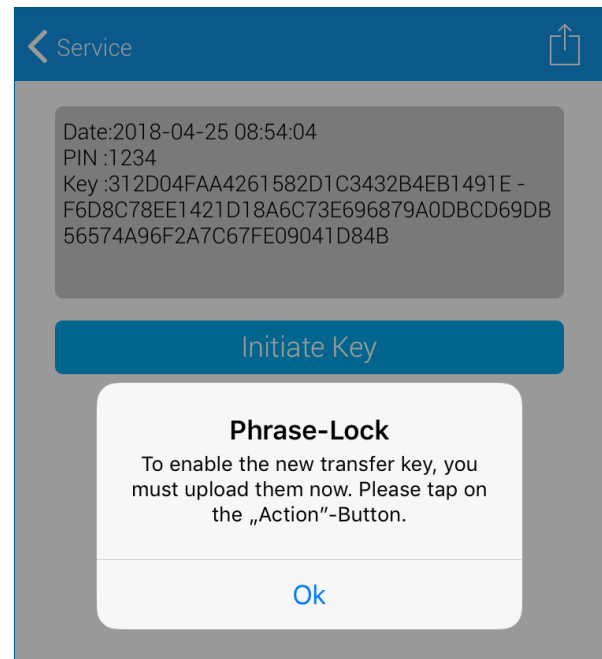
Now tap the **action button** at the top right. Please note the message window and acknowledge it after you have read it carefully.

The S-Key is ready now and you can start using the Enterprise Services.

*Please note: The Phrase-Lock Enterprise Services are services of the provider iPoxo IT GmbH, which are offered via its infrastructure (server). The S-Keys generated on the user's smartphone is stored **twice** encrypted in this infrastructure (database).*
*The first encryption is done with a key, which is calculated from the PIN code of the S-Key. This encryption is done exclusively on the user's smartphone. After transferring the already encrypted S-Key to the server, it is encrypted in the database for the second time.*

*It is therefore not possible for the provider iPoxo IT GmbH or its employees to read the S-Keys or synchronized login data of their customers in plain text without knowledge of the PIN code. Any data assigned to the user is only accessible via the user's USB-Key and the Enterprise Service login. There is a strict **client separation** of the data by the USB-Key. This restrictive encryption approach protects both, the user's data and ourselves, from being able to view our customers' data in plain text. It is technically impossible to decipher customer data without knowledge of the PIN-Code. Accordingly, we recommend a corresponding complexity for the PIN-Code.*
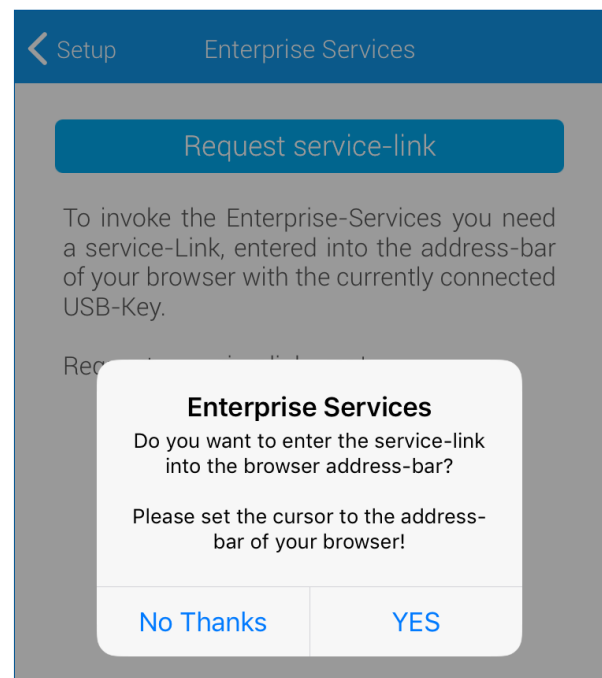
## Login to Enterprise Services

You can access the Enterprise Services via the **Enterprise Services (Enterprise Services Login)** menu item in the settings. Select this menu item and request a service link.

A message window then appears after that. Please read the note, open a browser window and point the cursor to the address line.

Now tap on **Yes** in the message window and the Enterprise Service login link is automatically entered in the address line of the browser.
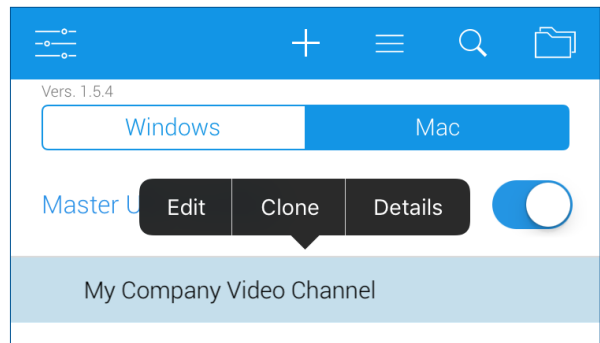
After the page has loaded, you will see the Enterprise Services menus corresponding to your license.
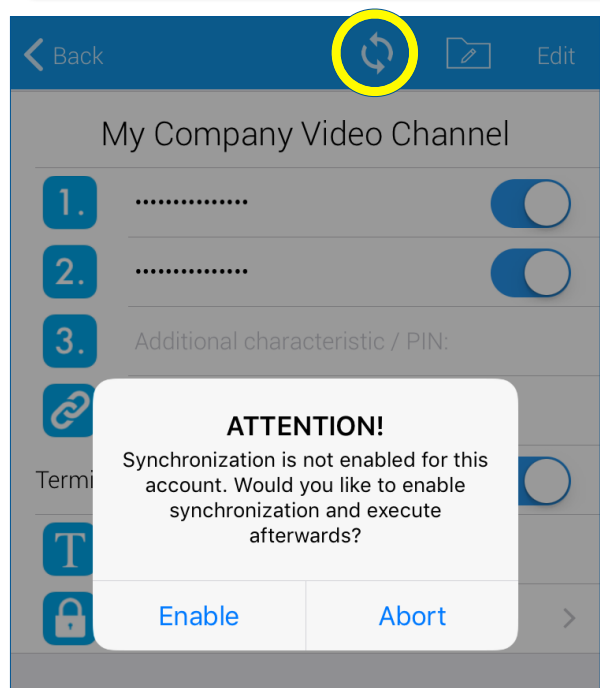
## Synchronizing login data from the smartphone

You can synchronize login data that are already on your smartphone. When a login data record is synchronized, it is stored twice encrypted on the servers of the service provider iPoxo IT GmbH.
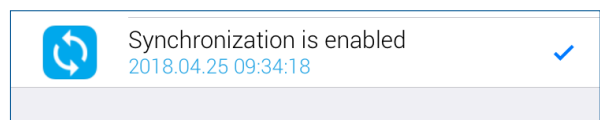
Now select the **Details menu** of a login record of your choice.

Tap the **synchronization button** and note the message window. Read its contents and activate or cancel the synchronization.

**Attention**: Synchronization can be deactivated by touching the „Synchronization is enabled" menu item. When deactivating, the login data will be deleted from the server, but will remain on the smartphone!

*Please note: The servers are located in a high security area of a data center in Vienna. All data that ultimately belongs to our customers are stored in this data center. Data center staff has physical access to the servers, but do not have gained any access rights. Even if a storage medium were to be removed without permission, it is not possible to read out login data due to the double encryption of customer data used.*

# Edit login data in the web interface

The web interface of the enterprise services was developed and tested with the latest versions of Google Chrome, Firefox and Safari. Microsoft's Internet Explorer and Edge Browser were not included in the development. In some cases, depending on the version and settings, these browsers may still work, but we do not offer support or troubleshooting for them.
We also only offer „Push-To-Login" plug-ins for the browsers mentioned above. For technical reasons, we did not consider Microsoft's browsers during development.

## The menus of the Enterprise Services

The web interface offers two main menus: **Login-Data** and **USB-Keys**. In the first tab, both main menus only display the USB key via which the service link was requested and entered. Here you can also see if and when the license of the enterprise services needs to be renewed. In most cases, however, the license is automatically renewed.
The second tab of the USB-Keys main menu lists the USB-Keys to which the license extends.



In the following, this manual only deals with the main menu item Login-Data and it is assumed that there is at least one additional USB-Key, to which login data can be assigned.

The **second** tab shows a login record (My Company Video Channel) that has already been synchronized via the smartphone.
The **second** field is used to edit the login data resp. to call the editor.
In the **third** field you can insert a note, which is then displayed on the phone. *This note cannot be edited on the phone, only in the Enterprise Services.*
The **fourth** field shows the unique ID of the respective login data record.
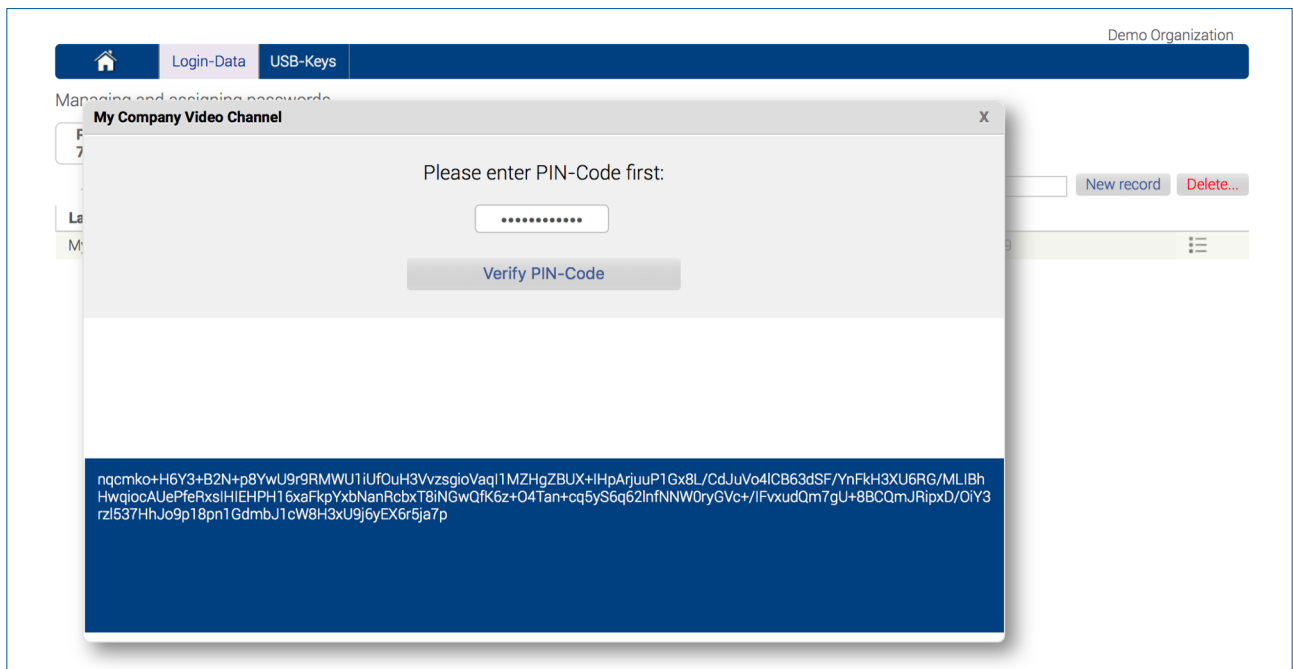The **fifth** field leads to further options.
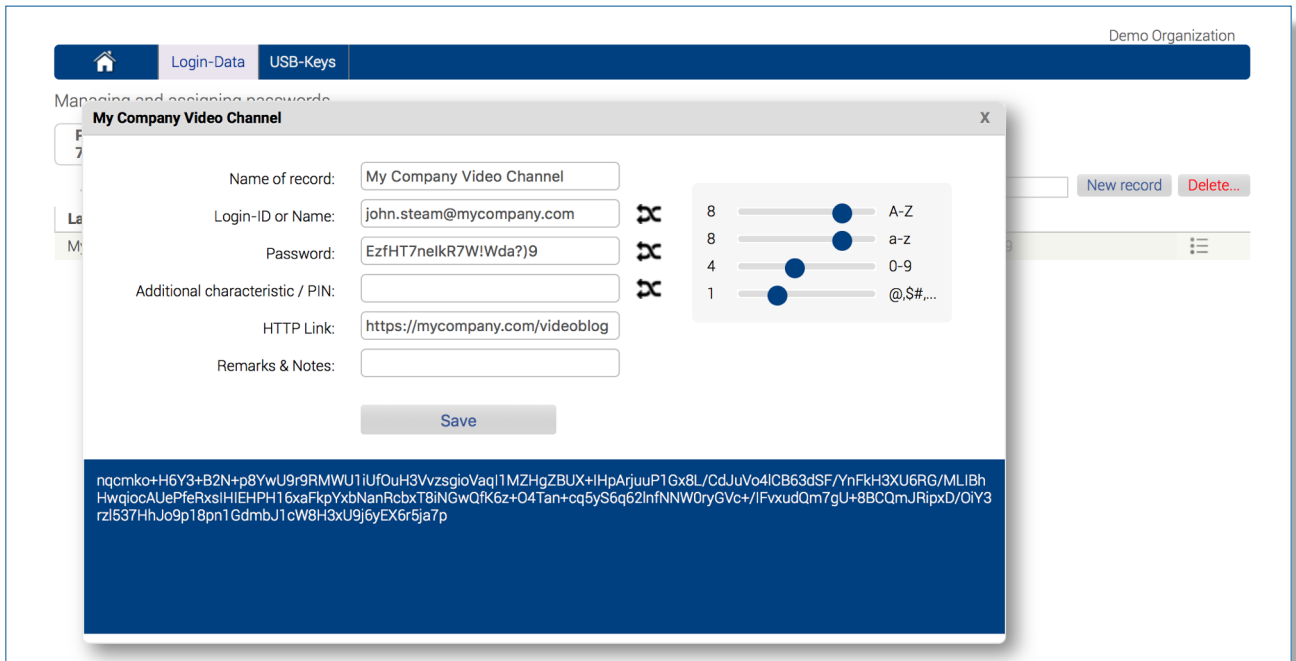
## Operation of the Enterprise Services masks

1) Main menu items can only be selected with a mouse click.

2) Within a main menu item the tabs can either be selected by mouse click or changed with Shift+arrow keys (left and right). However, keyboard control requires focus in one of the fields.

3) Within a tab the fields can be selected either by clicking or by using the arrow keys.

4) You can access the options menu of a login data record either by clicking on the field or by focusing on it with the arrow keys and pressing the ENTER key. You can return in the same way.

5) Changes and inputs in the list displays (e.g. name or comment of the login data) must be confirmed with ENTER. *Changing the field with the arrow keys or tabulator does not save any changes!*

## Editing a login record

In this step, the instructions require that there is already a data record under the Login data - Login data tab in the main menu that has been synchronised via the smartphone. In this example, the record is labeled **My Company Video Channel**.

Now focus on the second field with the lock symbol and press the ENTER button. Then the editor opens. In the editor you will be asked to enter the PIN code to decrypt the record for editing. You can see the encrypted record in the wide blue bar at the bottom of the editor. If the correct PIN code has been entered, the login data will be displayed as plain text and can be edited afterwards.

*Please note: The PIN code is now retained for the current session and does not have to be entered again if you want to edit further data records.*
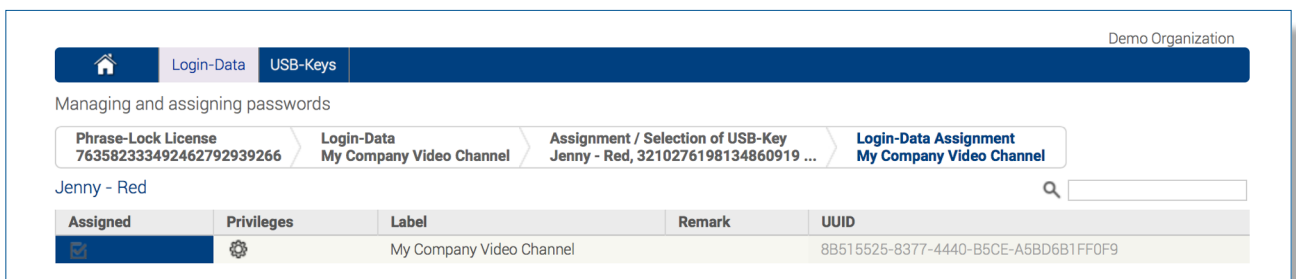*All encryption and decryption is done in JavaScript directly in the current window of your browser. PIN code and S-Key, in its decoded form, never leave the surface! This is guaranteed!*
*Browser plug-ins, also known as add-ons, browse websites for login names, passwords or other interesting information. Add-Blockers are also of this kind. Most of these little helpers are harmless and only do what they are meant to do. However, we would like to point out here that such plug-ins, depending on where they come from, can also contain a certain potential threat. Therefore, we ask all users of the Enterprise Services to think about it and look at the list of plug-ins and learn more about it. We cannot take the decision of which plug-ins should be trusted and which not.*
*As a rule of thumb for this decision: If you have enough confidence in the browser of your choice on a certain computer to carry out banking transactions or enter your credit card, the use of Phrase-Lock Enterprise Services should not pose any danger either!*

## Assigning login data

One of the main functions of Enterprise Services is the assignment of login data. In this example, login data of a fictitious **My Company Video Account** are assigned to a USB-Key called **Jenny Red**. **Jenny Red** is now able to transfer the login data to her smartphone using the **Assignments import** synchronization function. If a login data record does not yet exist, this data record is automatically assigned to the favorites.

## Rights of assigned login data

The creator of a login data record can change the rights of an assignment. The restriction of rights for third parties is always useful if the unwanted modification of an account is to be prevented. Whether an account is nevertheless changed in the target system cannot be prevented by this function.



## Synchronize changes

In the settings on the smartphone under **Extended Services** - apart from the menu option to log in for the Enterprise Services - there are three further menu items.

**Import private data:** If login data has been changed or added in the Enterprise Services, they can be read in or synchronized again. Data records that do not yet exist on the phone are imported and assigned to favorites without further notice. Changes to existing data records are displayed in a dialog and you can decide whether or not to accept the changes.

**Export private data:** Changes to login data made on the smartphone can be synchronized with this menu item. If necessary, the differences are displayed in a dialog and you can decide to synchronize or cancel the changes.

**Assignments import:** With this menu item you can synchronize those data records that have been assigned to you by another user.