



**uniqkey**

# Dashboard features

Uniqkey

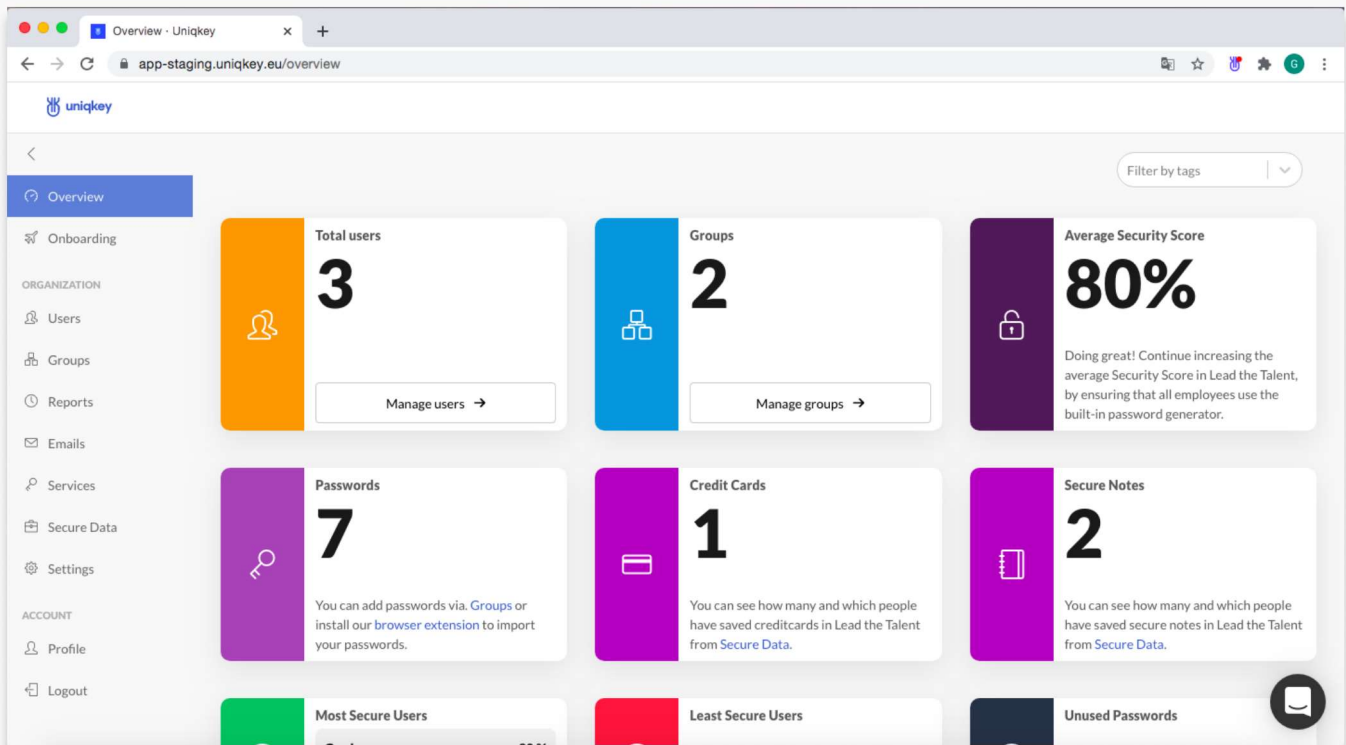
# Table of contents

1. Dashboard
2. Users and Groups
3. Reports
4. E-mails
5. Services and Secure data
6. Settings:

Business Information,  
Authorized Browser,  
AD and SCIM,  
Verified Domains

# Dashboard

The admin dashboard includes several different settings and useful features that can help improve the level of digital security in the organisation.



The front page of the dashboard provides a general overview of the different features in Uniqkey. You will find the various features in the menu on the left. On the front page, you will also be able to see data related to the use of Uniqkey in your organisation.

## Requirement specifications for Uniqkey

To make Uniqkey function optimally in your organisation, we recommend the following operating systems:

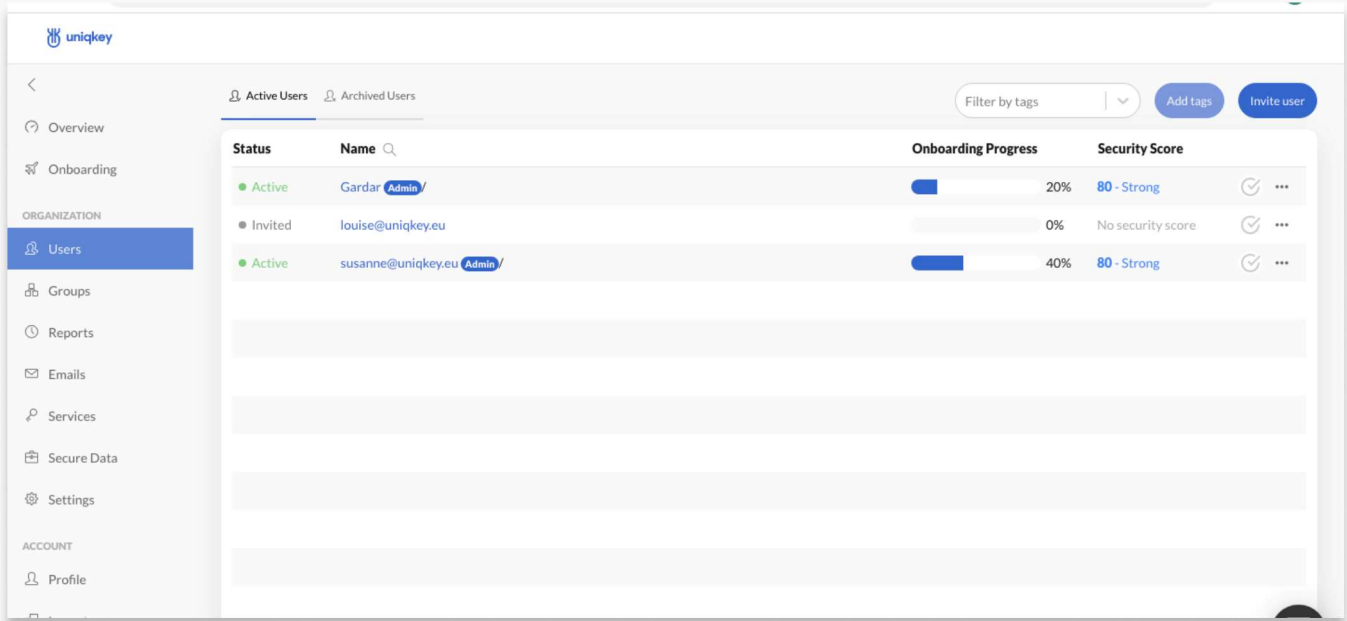
MacOS and iOS: Mojave, Catalina or Big Sur, iOS 10 - but 13 or later.

For Windows and Android: Windows 8 and Windows 10, Android 7.0 Nougat, Android 8.0 Oreo or later.

# Users and Group

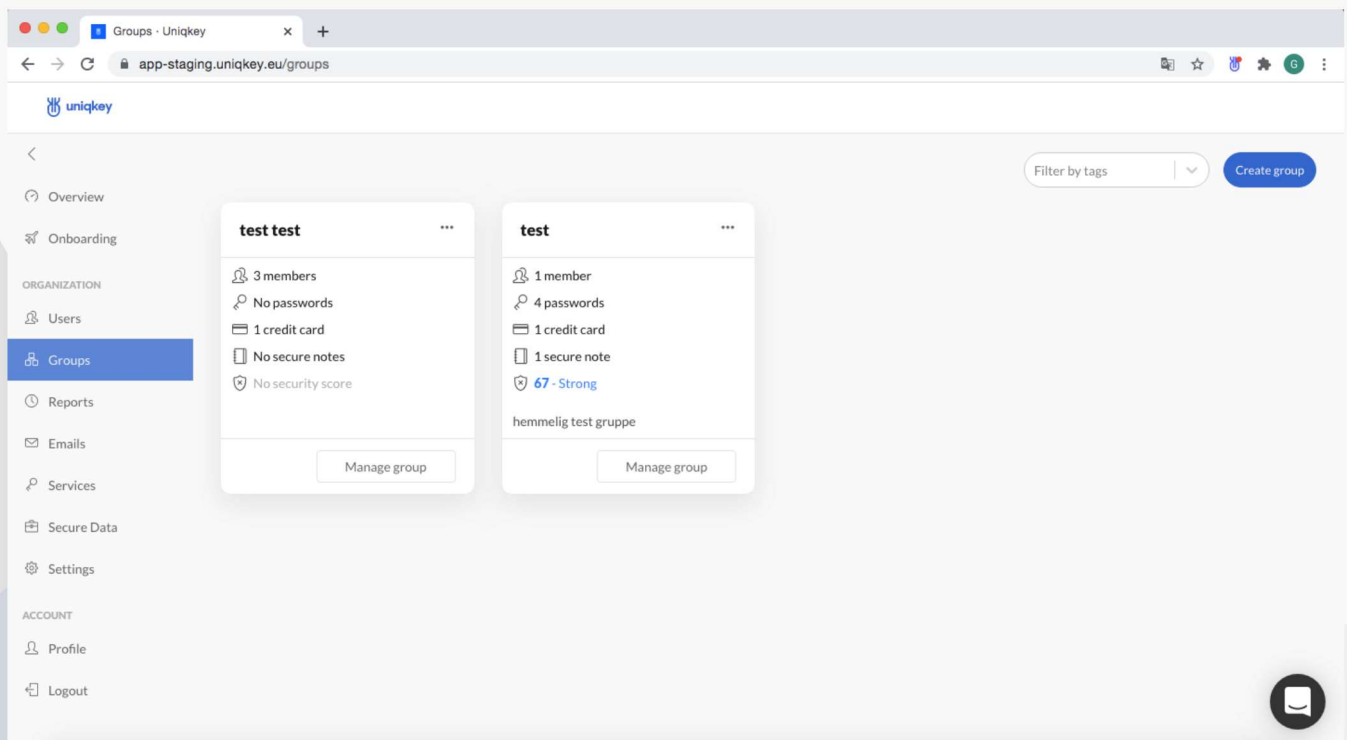
## Users:

Under “Users” you can find an overview of active users in Uniqkey. On the page Users, you can invite new users, grant admin privileges, or delete users.



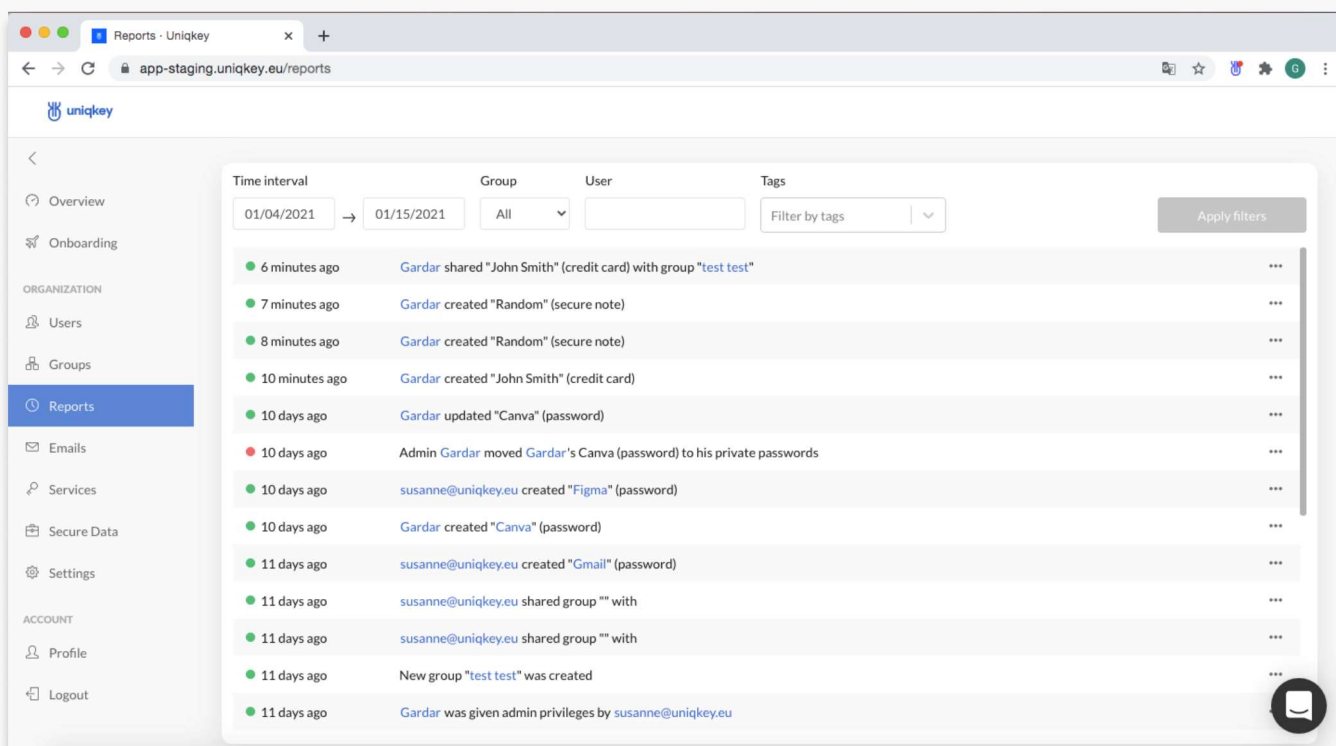
## Groups:

As an administrator, you can easily create groups in the dashboard. Groups make it possible to divide employees into e.g., departments or internal teams. As an administrator, you can give a group or team access to a specific account or service. The groups can have access to shared login credentials and accounts etc.



# Reports

Reports provides an overview of logins and activities with Uniqkey - for both users and administrators. You can view the reports at either a group level or for the individual users, and you can select the time frame for the report yourself.



## GDPR compliance with Uniqkey

The reports is effective in complying with the GDPR demands which states all companies must provide a complete 72 hours audit-log, if you have been hacked or are involved in a data leak.

The reports can also be used for internal security and view which logins have been accessed.

## E-mails

As an administrator, you can send feature e-mails to users directly in the admin dashboard. The feature e-mails can help inform the users about different security features in Uniqkey e.g., 2FA, password generator, etc. The e-mails also contain guides on how to quickly and easily set up the various features and thereby improve their own and the organisations online security.

If a user has a low security score, Uniqkey recommends that these feature emails be sent out to encourage the user to increase security around that user's login. You can send emails to specific groups or to individual users. All feature e-mails are available in both Danish and English.

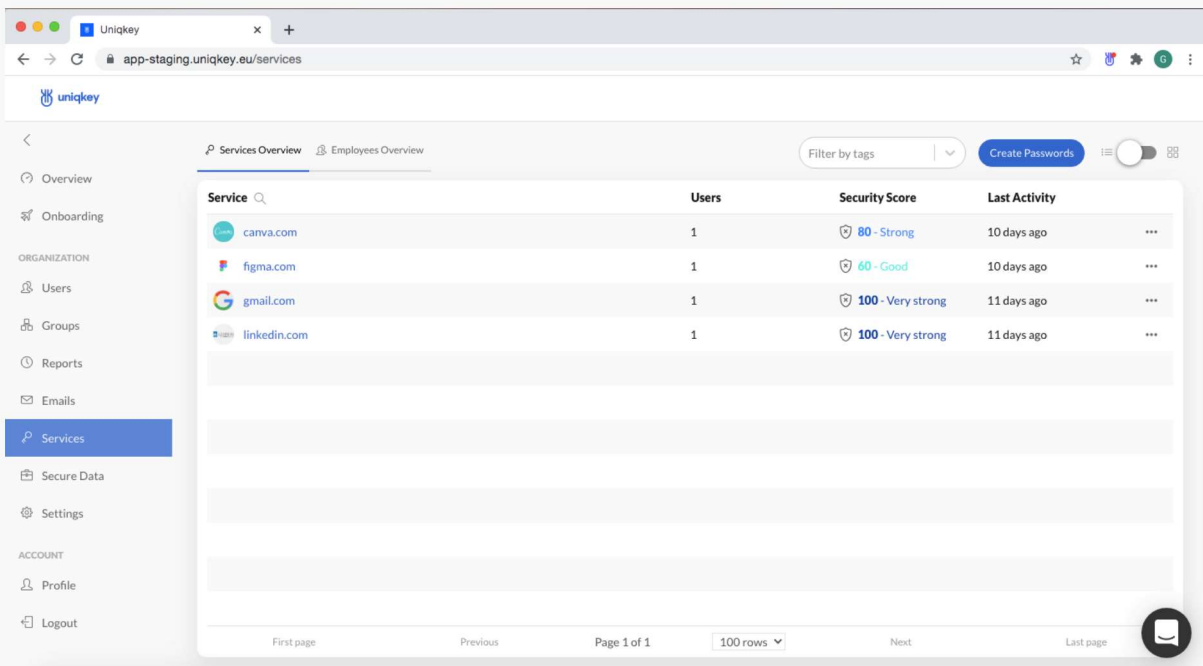


# Services and Secure data

## Services:

Under Services you can get an overview of the cloud services used by Uniqkey users in your organisation.

Also, you can see what time the service was last accessed, the number of users/licenses on the service, and the security strength of the login credentials. Private logins, which are stored in the users' private password manager, will not be visible in the dashboard.



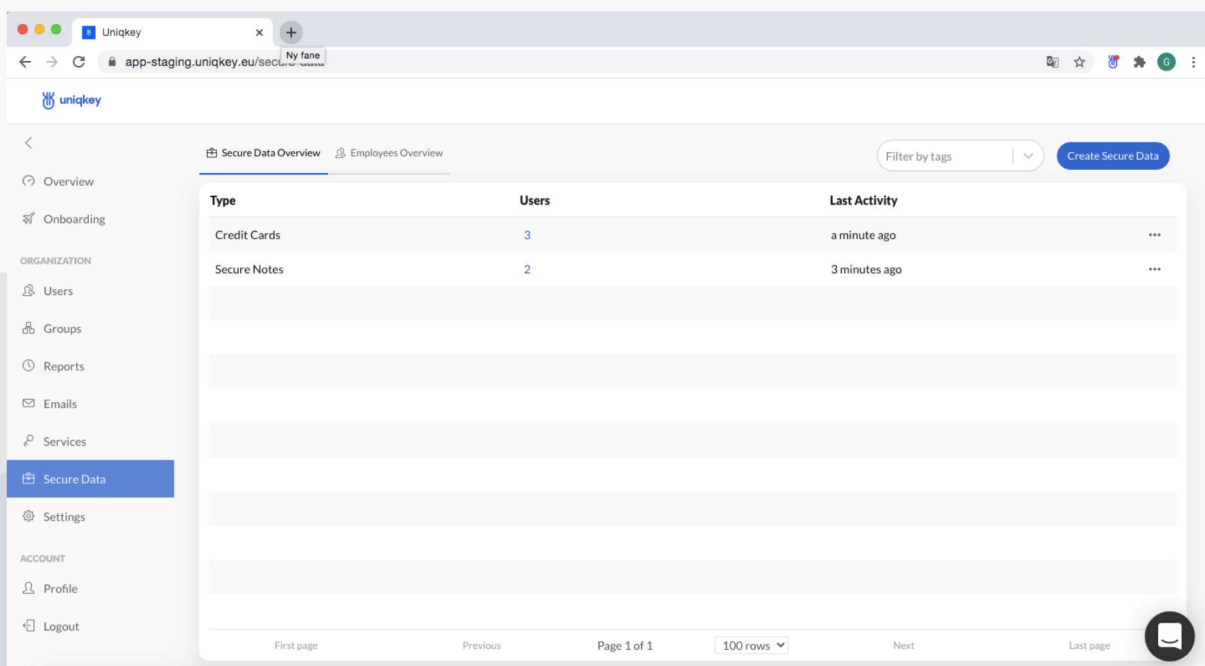
The screenshot shows the 'Services Overview' page in the Uniqkey dashboard. The page features a table with the following data:

Service	Users	Security Score	Last Activity
canva.com	1	80 - Strong	10 days ago
figma.com	1	60 - Good	10 days ago
gmail.com	1	100 - Very strong	11 days ago
linkedin.com	1	100 - Very strong	11 days ago

The dashboard includes a sidebar with navigation options like Overview, Onboarding, Users, Groups, Reports, Emails, Services (highlighted), Secure Data, Settings, Profile, and Logout. At the top right, there are filters and a 'Create Passwords' button. The bottom of the table shows pagination controls: 'Page 1 of 1', '100 rows', and 'Next'.

## Secure data:

Secure data relates to credit cards or secure notes. As an administrator, you can see how many users use these features, but you can also get a more detailed overview of the individual users.



The screenshot shows the 'Secure Data Overview' page in the Uniqkey dashboard. The page features a table with the following data:

Type	Users	Last Activity
Credit Cards	3	a minute ago
Secure Notes	2	3 minutes ago

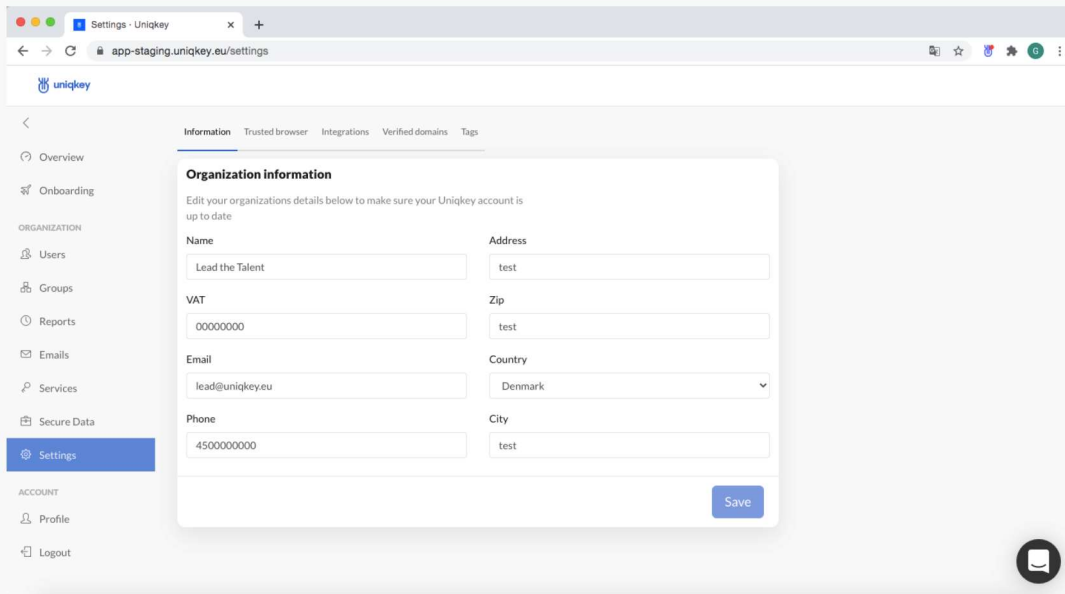
The dashboard includes a sidebar with navigation options like Overview, Onboarding, Users, Groups, Reports, Emails, Services, Secure Data (highlighted), Settings, Profile, and Logout. At the top right, there are filters and a 'Create Secure Data' button. The bottom of the table shows pagination controls: 'Page 1 of 1', '100 rows', and 'Next'.

# Settings

Under settings you find the tabs Company information, Trusted browser, Integration, Verified domains and tags.

## Company information:

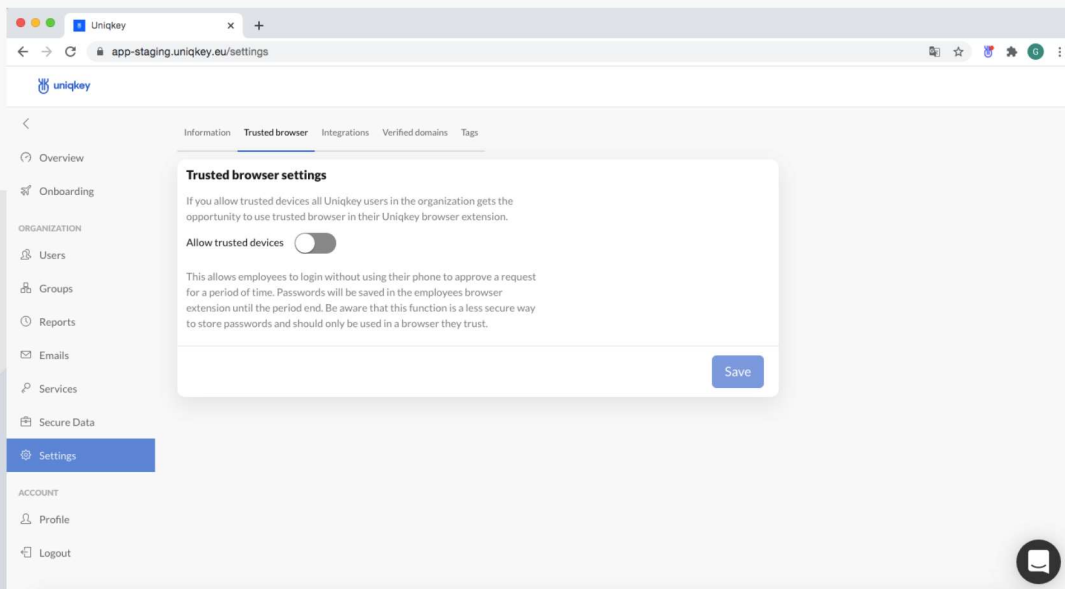
Company information is an overview of your company's general information, such as CVR number, contact information, etc.



## Trusted Browser

It may occur that users will be bothered by having to approve every single login with their smartphone. That is why we have developed the trusted browser feature. This feature allows users to be logged in automatically for a given period e.g., 08.00-16.00. During this time, the passwords will be stored locally in the user's browser, and users will therefore not need to authenticate logins from their smartphone.

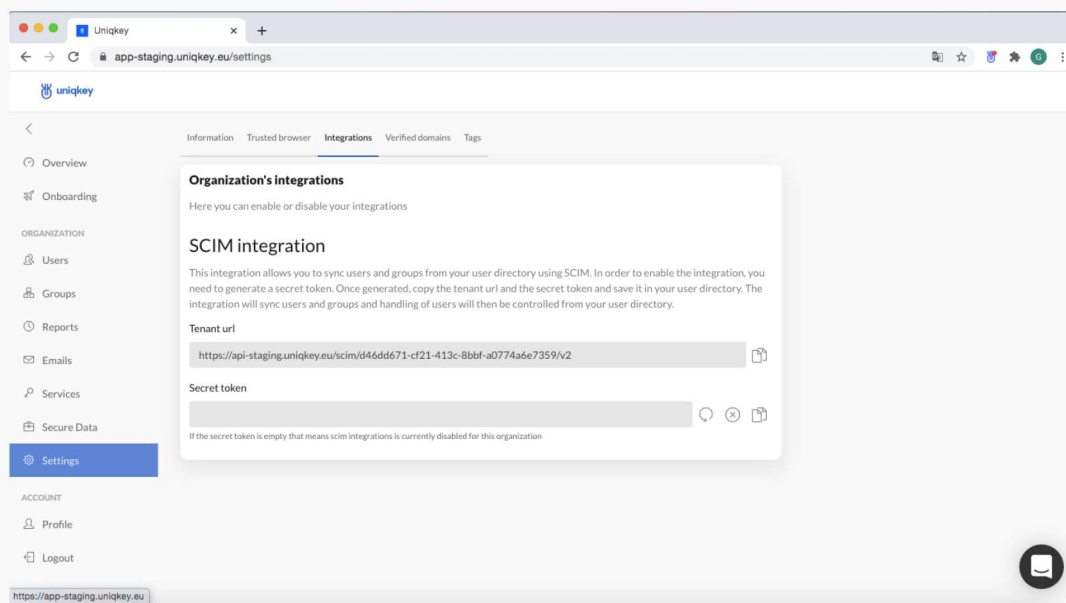
For security reasons, Uniqkey does not recommend using this feature. However, after high demand, it is an option to enable this feature.





## AD and SCIM

Uniqkey can be rolled out easily to all users in your organisation with Azure Active Directory and SCIM 2.0. This step generally happens in the technical rollout phase, and there is a detailed guide that describes how to do the integration.



## Verificerede domains:

Verified domains display a list of the domains created by the company. These registered domains define where a login is stored in the user's password manager. All logins created with e.g., `name@yourorganisation.com` will be stored under company logins and will not be able to be transferred to the private password manager.

These domains can only be created by Uniqkey. If the company wants to create more domains, please contact the administrator Uniqkey.

