



Dashboard

Administrator guide for Uniqkey's dashboard

Table of contents

As an administrator you can use this guide to become acquainted with the Admin Dashboard. The guide describes various features and functions that can be used to improve the digital security level in your organisation.

1. Invite new users
 - a. Add administrators
2. Create groups
 - a. Adding accounts to groups
3. Onboarding in Uniqkey
4. Offboarding of employees with transfer of login ownership
5. Control over employee access to company accounts
 - a. Overview of cloud services
6. E-mails
7. Activation of trusted browser
8. Restrictions:
 - a. Geo restriction
 - b. IP restriction
 - c. Time restriction
 - d. Copy restriction
9. Reports



1 Invite users

Note: If you have integrated Uniqkey with AD using SCIM 2.0 the company's users will automatically added to invited users.

To invite new users, in the Dashboard, select users.

Invite new users:

- To invite new users, in the Dashboard, select users
- Click "Invite new user" and enter the e-mail-address of the employee.
- Click "Send invitation"

Subsequently, the employee will receive an activation e-mail with a guide to getting started with Uniqkey.



1.a Add administrators

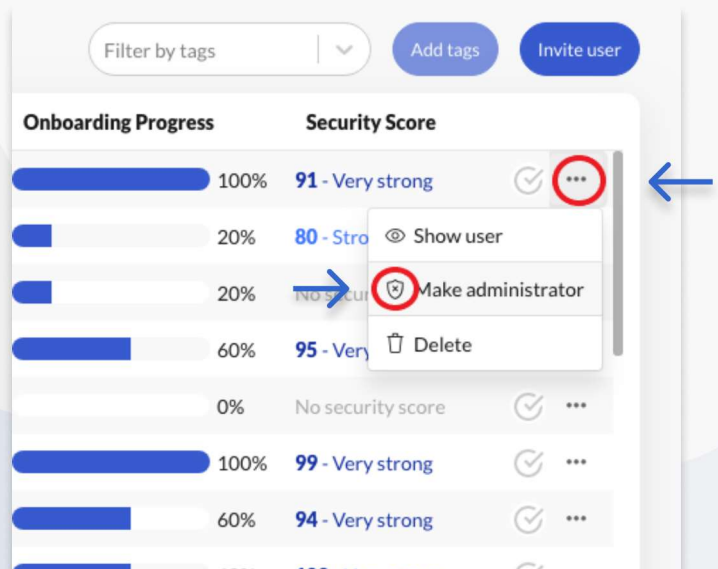
It is important to select several employees for the role of administrator, as Uniqkey can in no way reactivate or reset access to the Dashboard for the company.

The administrators in the company are the only ones who can access the company's data.

In order to give a Uniqkey user administrator rights, the user must have an active Uniqkey account.

Add an administrator:

- Clicking on "Users"
- Select the user you want to make an admin
- Click on the three dots and select "make administrator"



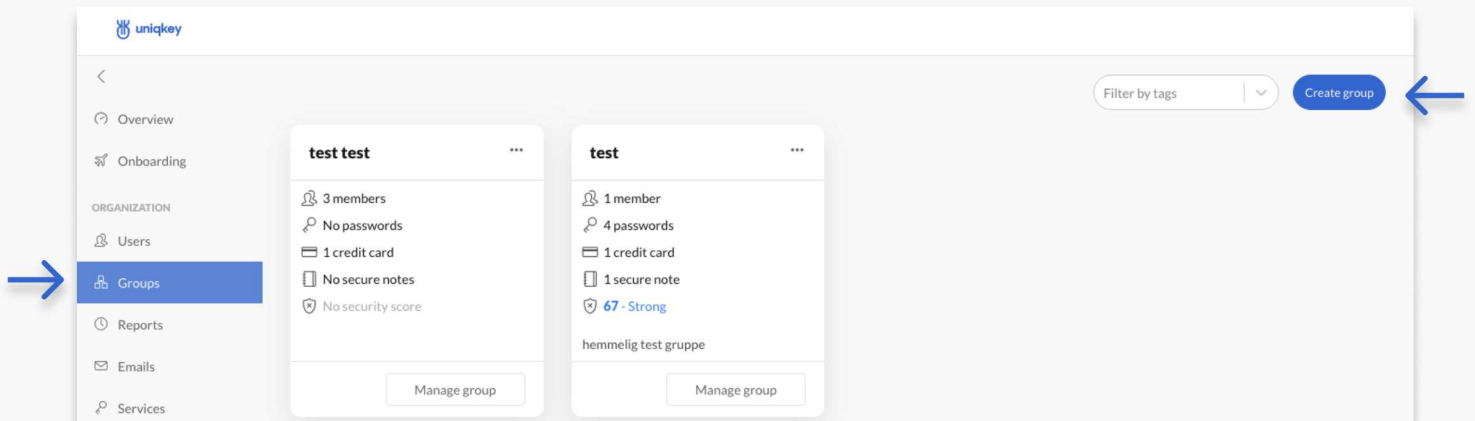
2 Create groups

Groups is a function that makes it possible to divide employees into teams or departments and there by easily and quickly give the entire group the necessary rights, access and permits.

How to add users to groups:

- Click “Groups” in the side sidebar or “Go to group” on the homepage
- Create or find the group you want to add an employee to and click on “Manage groups”
- Click “Invite users”
- Insert the user’s e-mail and press “Invite”

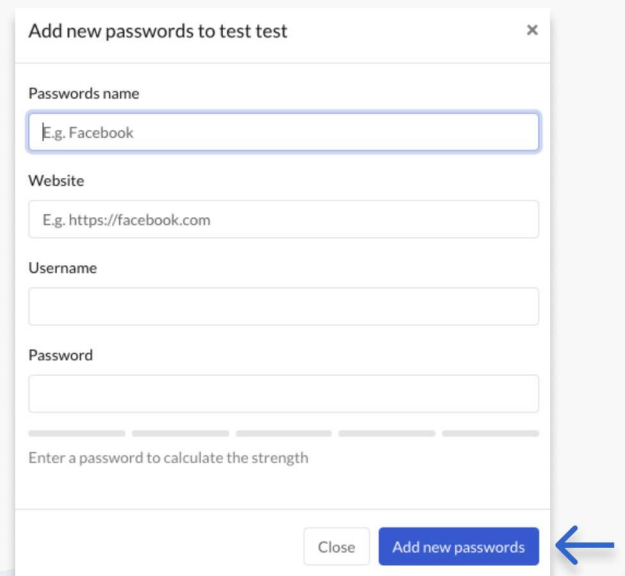
The user is now invited



As an administrator, you can give a group or team access to a specific account or service. This gives the whole group access to the account at the same time.

2.a Add new passwords to groups :

- Access “Passwords” in the group
- Click “add account”
- Add account name, web address, username and password
- Press “Add new password”
- You will receive a notification on your Uniqkey mobile app. press “Accept”



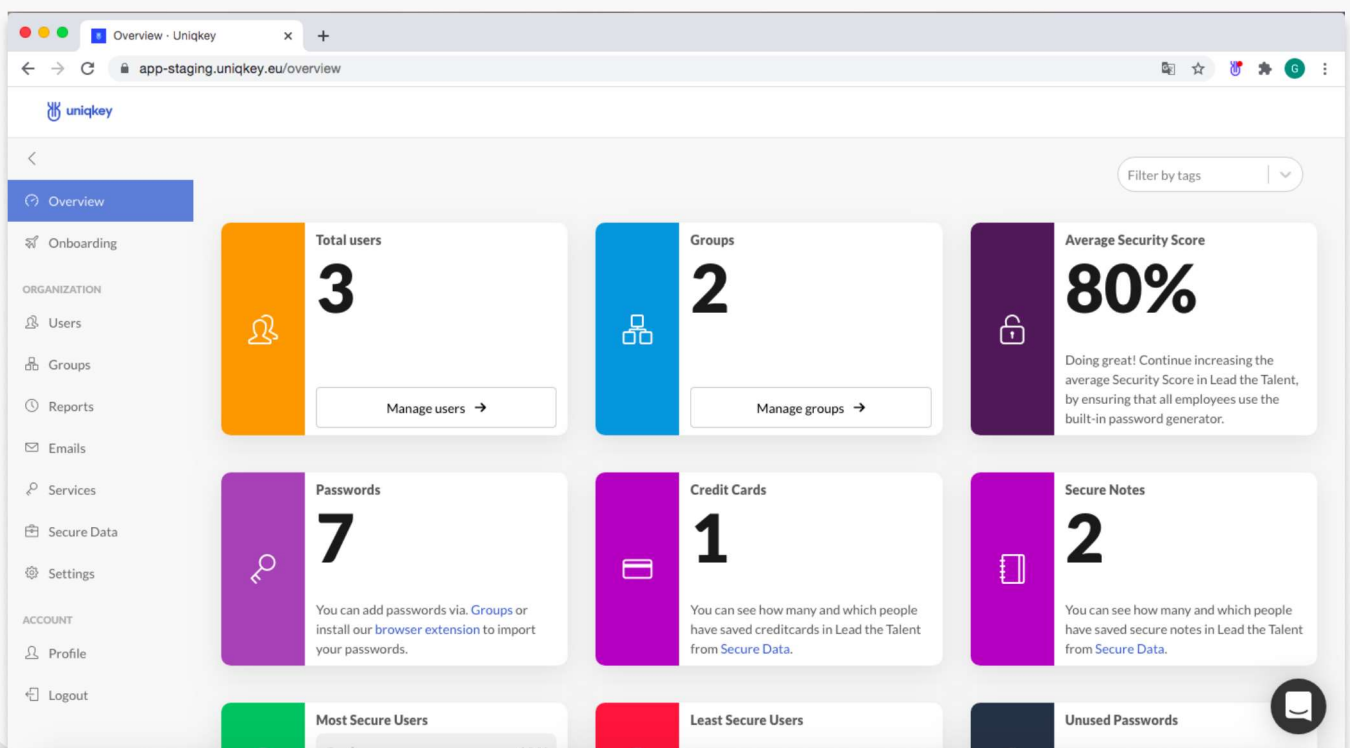
You also have the option of sharing an account you have already created in Uniqkey with a group you are a part of. This can be done both from the app and from the browser extension under the individual account.

3 Get a good overview of the users onboarding

In the onboarding and activation phase of users in Uniqkey, there are several features and criteria you can measure. To get the best possible onboarding and activation flow with Uniqkey, we recommend that you only set up a few onboarding criteria to begin with. The reason for this recommendation is to give administrators and users a chance to become familiar with the system.

As more users become more familiar and confident with using the system, you can set up more criteria and measure which functions are used Uniqkey such as 2FA in Microsoft etc.

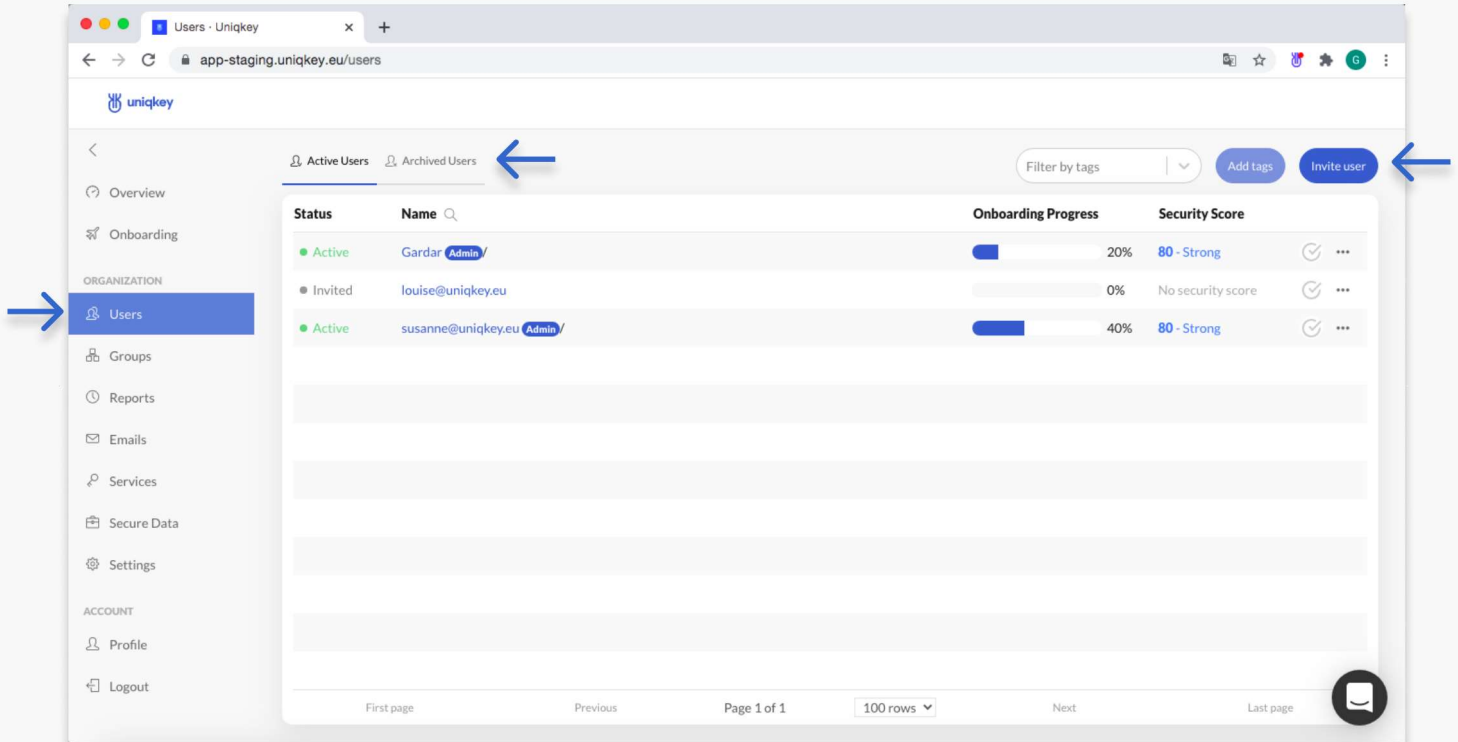
You will be able to measure how successful your onboarding is, both at an individual and a group level.



4 Off boarding of employees and transfer of login ownership

When an employee stops, it becomes easier for the company to get an overview which cloud services are used in the organisation and get an overview of which employees have active licenses and logins for the services.

If/when a user for some reason stops working for the organisation it will be easy to remove their access to organisational cloud solutions and systems with Uniqkey. If the company needs passwords from their former employee, the administrator can access the dashboard move the credentials and then delete accounts.



Status	Name	Onboarding Progress	Security Score
Active	Gardar Admin	20%	80 - Strong
Invited	louise@uniqkey.eu	0%	No security score
Active	susanne@uniqkey.eu Admin	40%	80 - Strong

Offboard a user:

To delete a user in Uniqkey, you must be logged in to the administrator Dashboard.

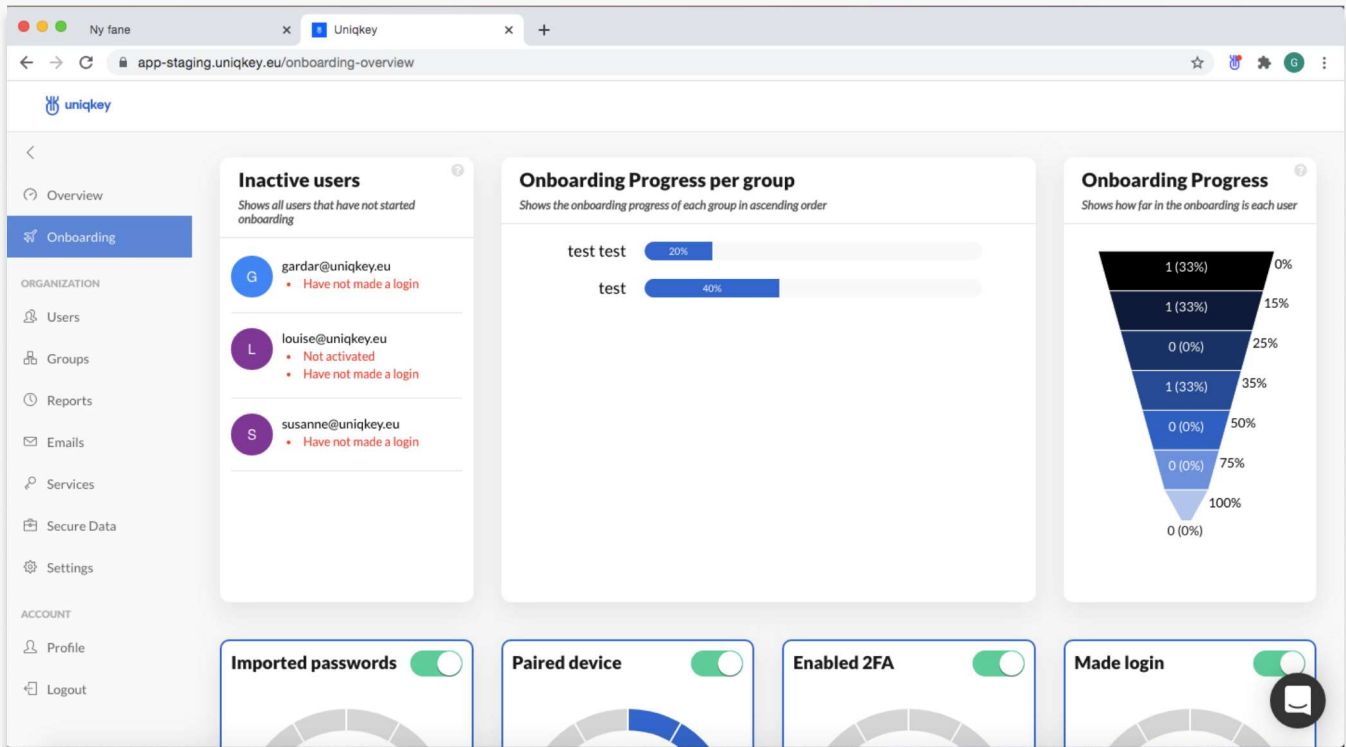
- Select "Users" in the menu.
- Find the user you would like to remove and click the three dots to the right of their name.
- Click remove user and Delete.
- The user will now be archived under Archived Users in the Dashboard.

Archived users:

When a user account has been deleted the administrators can retrieve the former employee's company passwords and move the passwords to other users or groups in the company. This feature ensures that logins to various cloud services are not lost and that the company can log on to its service, cancel licenses and change 2FA settings.

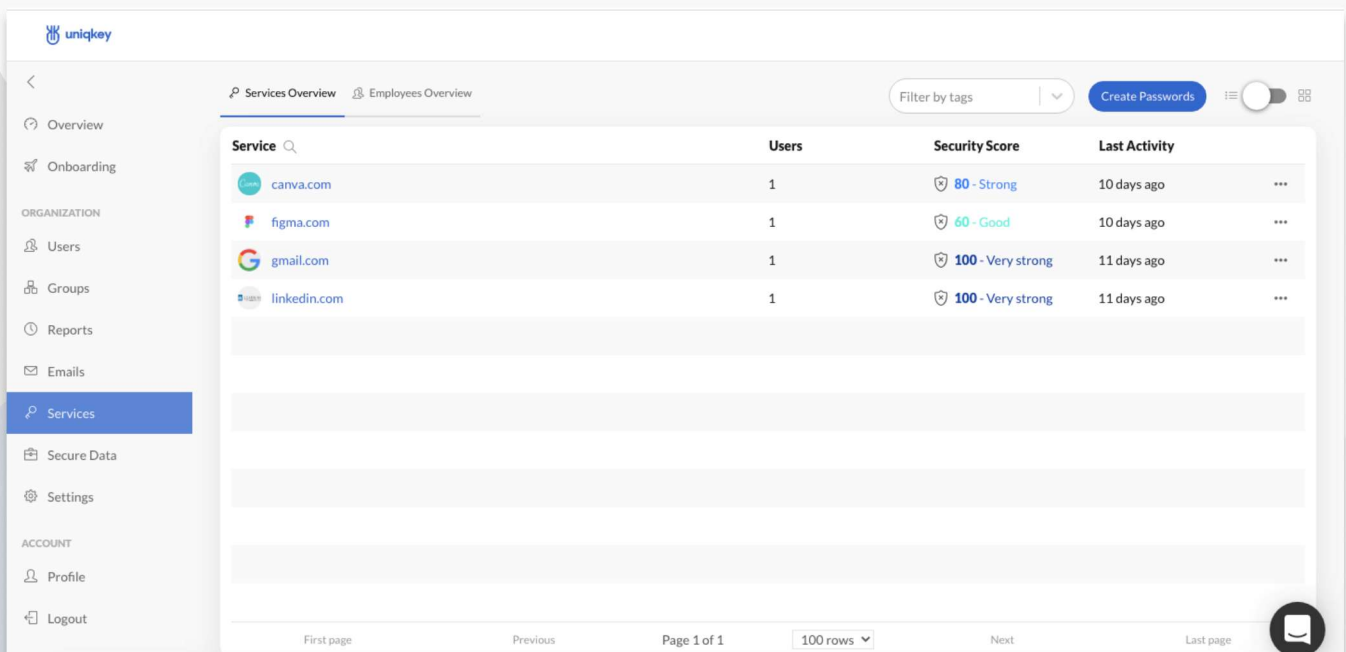
5 Centralised overview and control of employee access to company accounts.

Using Uniqkey makes it easier to control which employees have access to the various systems and company logins. It will also make access control for business-critical systems easier. With the centralised overview and easy access control management it makes it easier for you as an admin to ensure that the most critical systems are protected and only available to the relevant users.



5.a Overview of cloud services

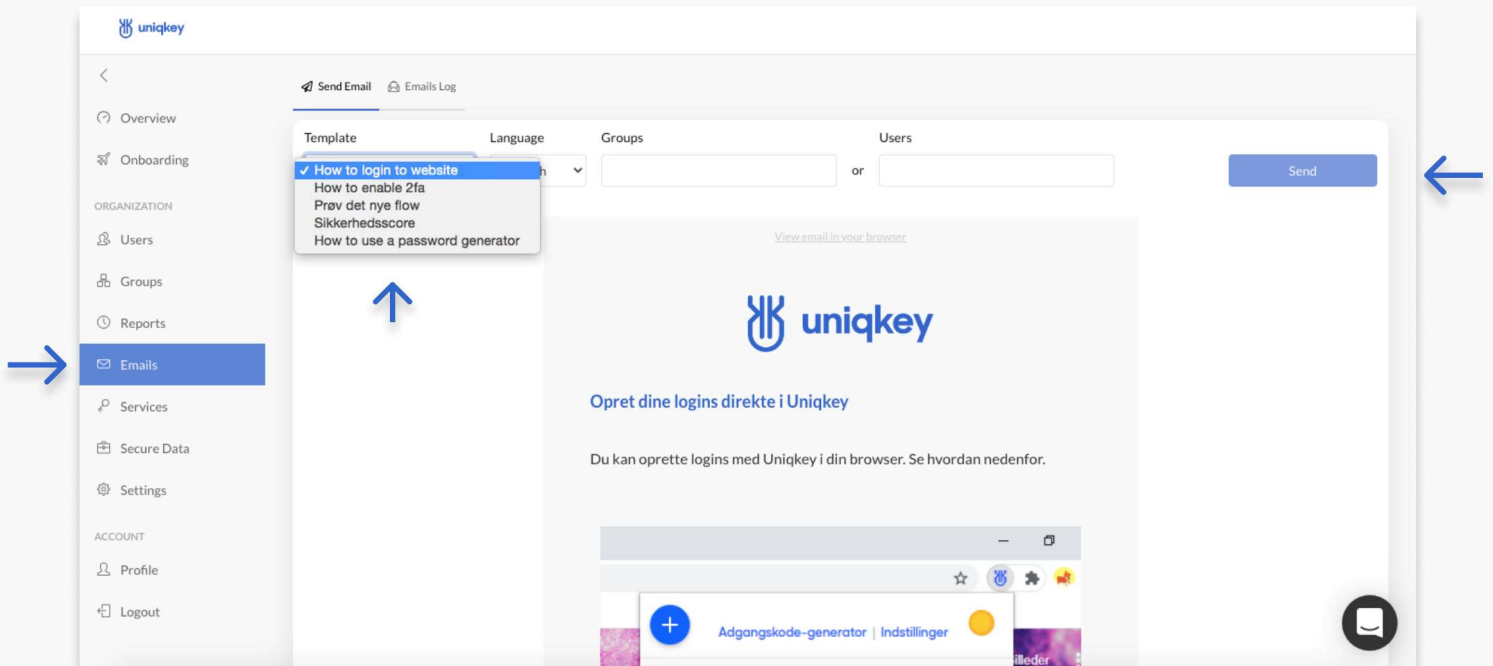
As an admin, you can get an overview of the cloud services that are used in the company. It is also possible to see which services are being used as well as active licenses and invited users.



6 E-mails in the Dashboard

As an administrator, you can send out e-mails to users directly from the Dashboard e.g., reminder or feature e-mails. The feature mails have been created to help inform users on how to increase their online security through e.g., 2FA, password generator, etc.

All feature e-mails are available in both Danish and English in your Dashboard.



How to send E-mails from the dashboard:

- Click on “E-mails” in the menu
- Choose mail template
- Choose “Language”
- Select the user/group who you want to send the mail to.
- Press “Send”

Uniqkey recommends

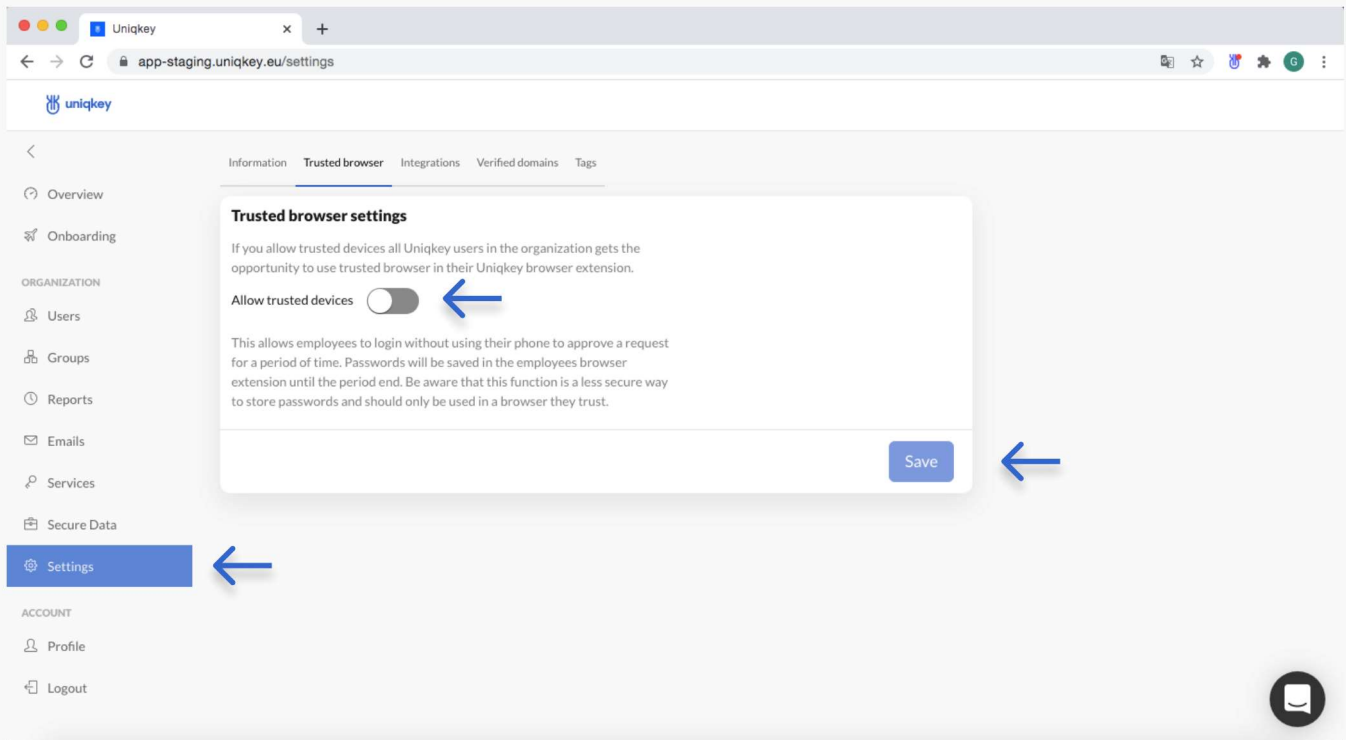
If a user has a low security score, Uniqkey recommends that the e-mails are sent out to encourage the user to increase security around that user's logins. You can send e-mails to specific groups or to individual users.

7 Activation of Trusted browser

It may occur that some users will be bothered by having to approve every single login with their smartphone. Therefore, we have developed the function Trusted browser: It is a function that means that the user is not forced to approve logins from their smartphone for a given period, e.g., 08.00-16.00. During this time, the passwords will be stored locally in the user's browser.

Uniqkey anbefaler af sikkerhedsmæssige årsager ikke at man anvender denne funktion. Efter stor efterspørgsel er det dog en mulighed at aktivere denne funktion.

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



The screenshot shows a web browser window with the URL `app-staging.uniqkey.eu/settings`. The page displays the 'Trusted browser settings' section. The 'Allow trusted devices' toggle is currently turned off. A blue arrow points to the 'Settings' menu item on the left sidebar. Another blue arrow points to the 'Allow trusted devices' toggle. A third blue arrow points to the 'Save' button at the bottom right of the settings card. The settings card contains the following text: 'Trusted browser settings', 'If you allow trusted devices all Uniqkey users in the organization gets the opportunity to use trusted browser in their Uniqkey browser extension.', 'Allow trusted devices' (with a toggle switch), and 'This allows employees to login without using their phone to approve a request for a period of time. Passwords will be saved in the employees browser extension until the period end. Be aware that this function is a less secure way to store passwords and should only be used in a browser they trust.'

8 Restrictions

It is possible to set up restrictions that can secure the company via geographical location, IP-address and time restrictions. For example, you can decide whether employees can access various company accounts outside the workplace or only from the workplace.

These restrictions can be set up for groups in the company. With group restrictions, you as an IT administrator can decide where and when specific accounts may be accessed.

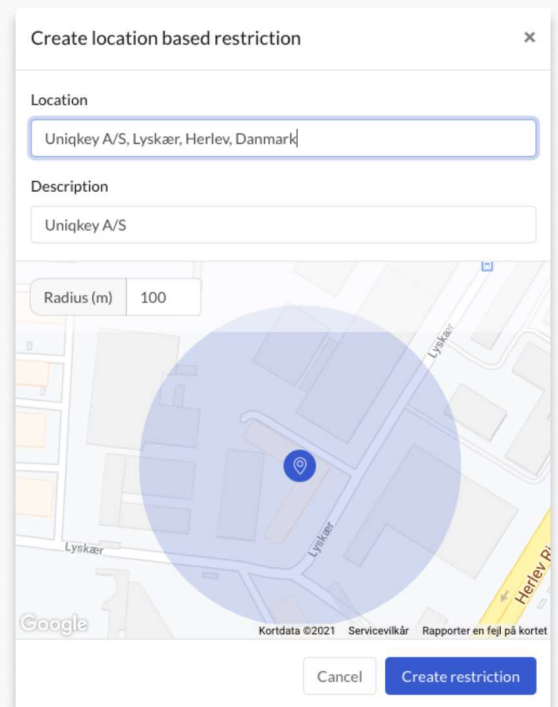
If you add more than one of the same types of restriction to a group, only one of the two restrictions of the same type needs to be met. i.e. If you have set two Geo restrictions, for example for your offices in both Aarhus and Copenhagen, it is of course only necessary to meet one location requirement.

8.a Geo restriction

The geo restriction function defines a physical location where a group's accounts or specific logins can be used. If the user has not enabled location services, it will not be possible to access accounts with geo-restrictions.

Create a geo restriction:

- Access groups in the menu
- Choose “manage group”
- Select the geo restriction
- Choose location and description
- Press “Create restriction”



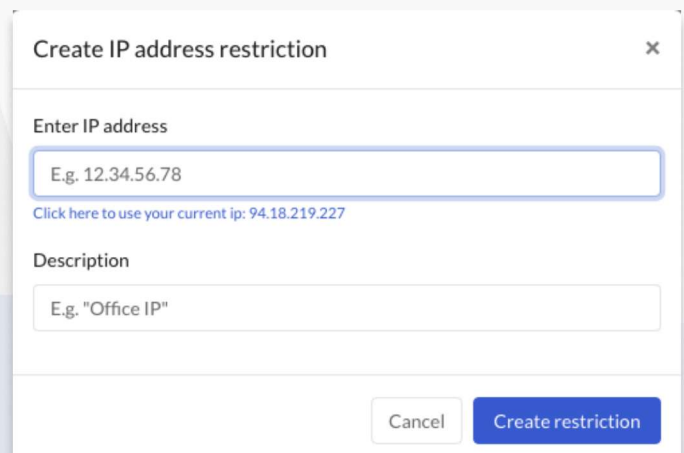
8.b IP restriction

You can create IP restriction, and define which IP addresses it should be possible to log in to different services and group accounts.

The IP address to be entered must be a CIDR address.

Create an IP restriction:

- Access groups in the menu
- Choose “manage group”
- Select the IP restriction
- Enter IP and description
- Press “Create restriction”

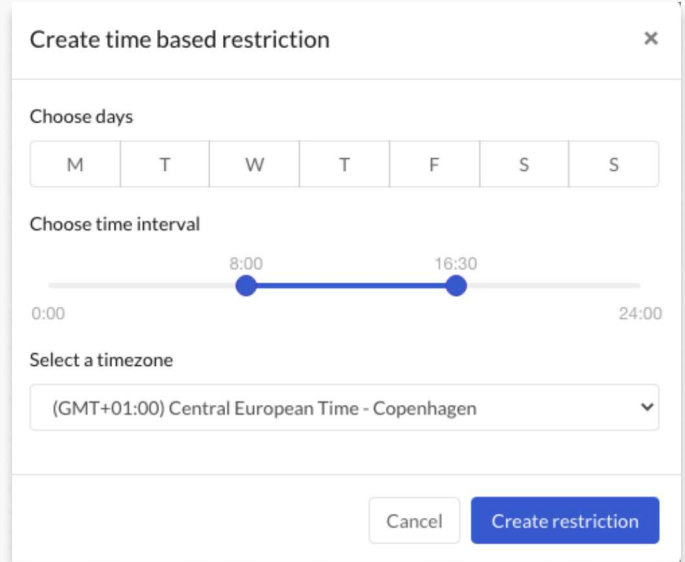


8.c Time restriction

As an additional security measure, you can decide which days and during which periods special logins and group accounts can be used.

Create a time restriction:

- Access groups in the menu
- Choose “manage group”
- Select the restriction
- Choose days, time interval and the timezone
- Press “Create restriction”

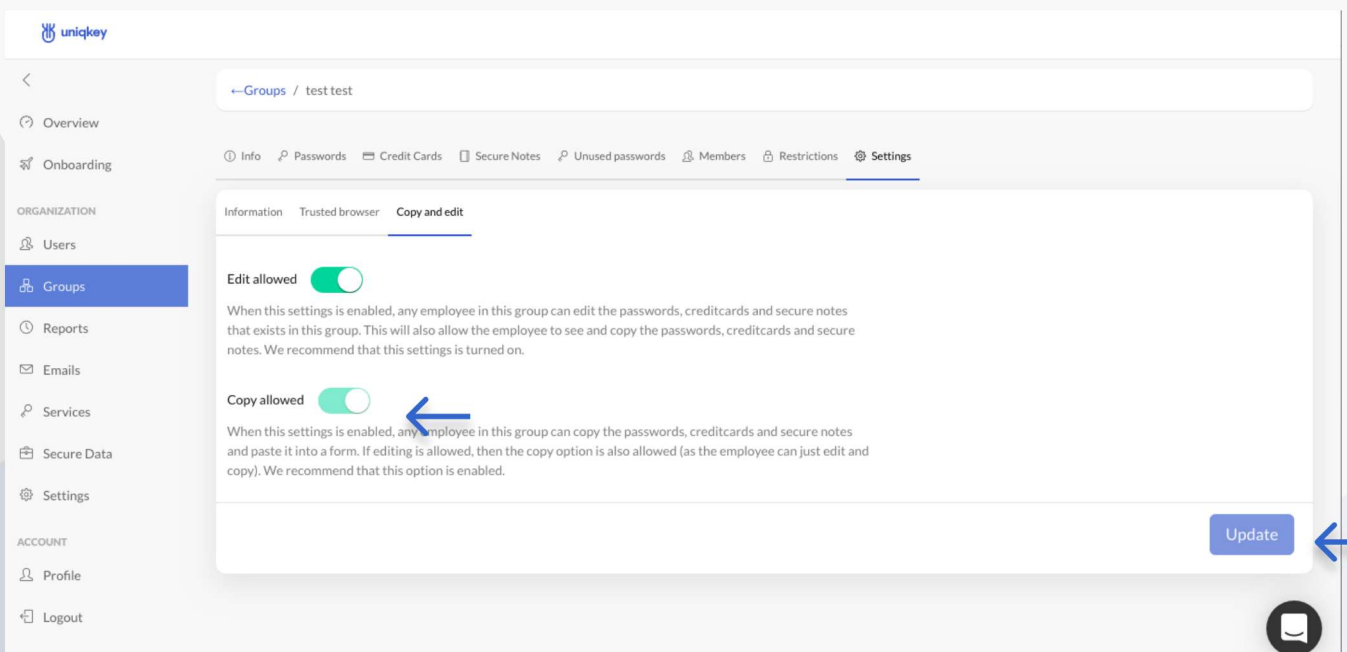


8.d Copy restriction

Under settings it is possible to create copy restrictions. If “copy allowed” is disabled by the administrator it will not be possible for the user to view or copy shared passwords.

Create a copy restriction:

- Under “Groups” go to “Settings”
- Choose “Copy and edit”
- Choose “Copy allowed”
- Press “Update”



The screenshot shows the Uniqkey interface with a sidebar on the left containing 'Groups' and 'Settings'. The main content area is titled 'Groups / test test' and has a navigation bar with 'Info', 'Passwords', 'Credit Cards', 'Secure Notes', 'Unused passwords', 'Members', 'Restrictions', and 'Settings'. Under 'Settings', there are three tabs: 'Information', 'Trusted browser', and 'Copy and edit'. The 'Copy and edit' tab is active and shows two settings:

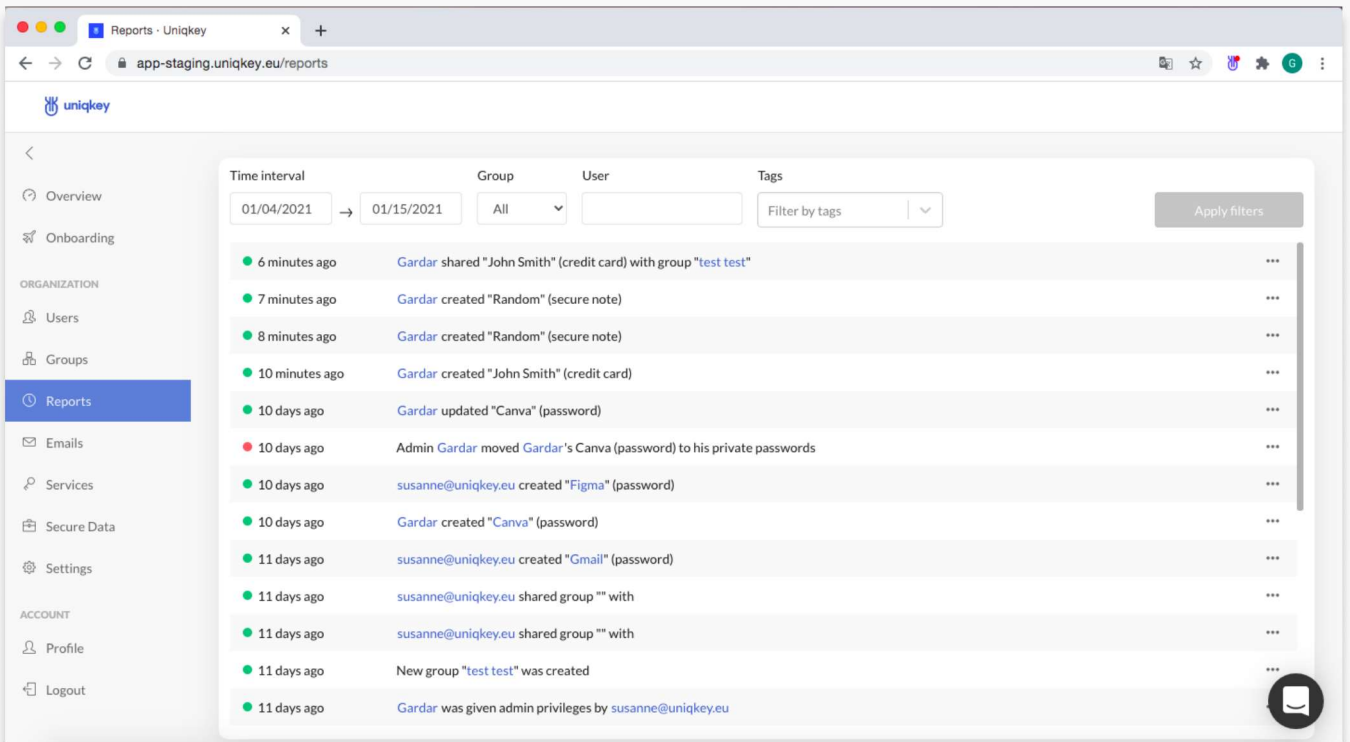
- Edit allowed:** A green toggle switch is turned on. Below it, text reads: "When this settings is enabled, any employee in this group can edit the passwords, creditcards and secure notes that exists in this group. This will also allow the employee to see and copy the passwords, creditcards and secure notes. We recommend that this settings is turned on."
- Copy allowed:** A green toggle switch is turned on. Below it, text reads: "When this settings is enabled, any employee in this group can copy the passwords, creditcards and secure notes and paste it into a form. If editing is allowed, then the copy option is also allowed (as the employee can just edit and copy). We recommend that this option is enabled."

At the bottom right of the settings panel, there is a blue 'Update' button.

9 Reports

The reports provides an overview of logins and activities in Uniqkey - the log shows the activities of both users and administrators.

You can view reports a group level or for the individual users, you can filter the time interval for the reports.



The screenshot shows the Uniqkey Reports interface. The left sidebar contains navigation options: Overview, Onboarding, ORGANIZATION (Users, Groups, Reports, Emails, Services, Secure Data, Settings), and ACCOUNT (Profile, Logout). The Reports section is active. The main content area features a filter bar with the following settings: Time interval (01/04/2021 to 01/15/2021), Group (All), User (empty), and Tags (Filter by tags). Below the filter bar is a list of activities:

Time	Activity	Action
6 minutes ago	Gardar shared "John Smith" (credit card) with group "test test"	...
7 minutes ago	Gardar created "Random" (secure note)	...
8 minutes ago	Gardar created "Random" (secure note)	...
10 minutes ago	Gardar created "John Smith" (credit card)	...
10 days ago	Gardar updated "Canva" (password)	...
10 days ago	Admin Gardar moved Gardar's Canva (password) to his private passwords	...
10 days ago	susanne@uniqkey.eu created "Figma" (password)	...
10 days ago	Gardar created "Canva" (password)	...
11 days ago	susanne@uniqkey.eu created "Gmail" (password)	...
11 days ago	susanne@uniqkey.eu shared group "" with	...
11 days ago	susanne@uniqkey.eu shared group "" with	...
11 days ago	New group "test test" was created	...
11 days ago	Gardar was given admin privileges by susanne@uniqkey.eu	...

GDPR compliance with Uniqkey

With GDPR it is a legal requirement that all companies must be able to deliver a complete systems Audit Log within 72 hours of a data breach. The audit log can be used internally for security checks. The audit log should for security reasons, always be able to be easy to access in the event of a data breach. With Uniqkey you automatically have an audit log report.