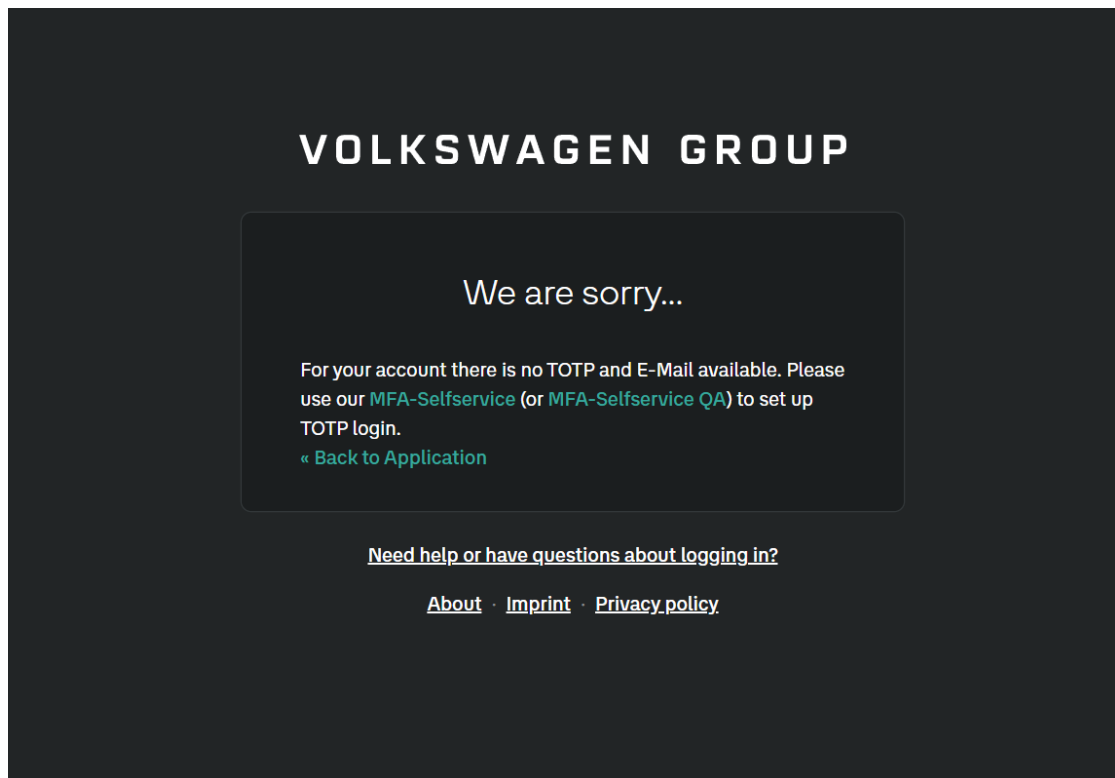



CloudIDP MFA (TOTP) Setup Without PKI and Email

- Normally, registration for the TOTP method starts automatically when you access a web application that requires strong authentication (e.g., Success Factors).
- If you do **not** have a company email address or PKI card, you need support from a direct colleague or supervisor with a PKI card, as the registration process must be secured. That's why you will see the following error page.



- Ask a colleague from your (sub-)department with a PKI card to enter your UserID at <https://mfa.idp.cloud.vwgroup.com> (button “Allow TOTP-Setup without email”) to enable your TOTP setup.

CloudIDP MFA-Selfservice [Logout](#)



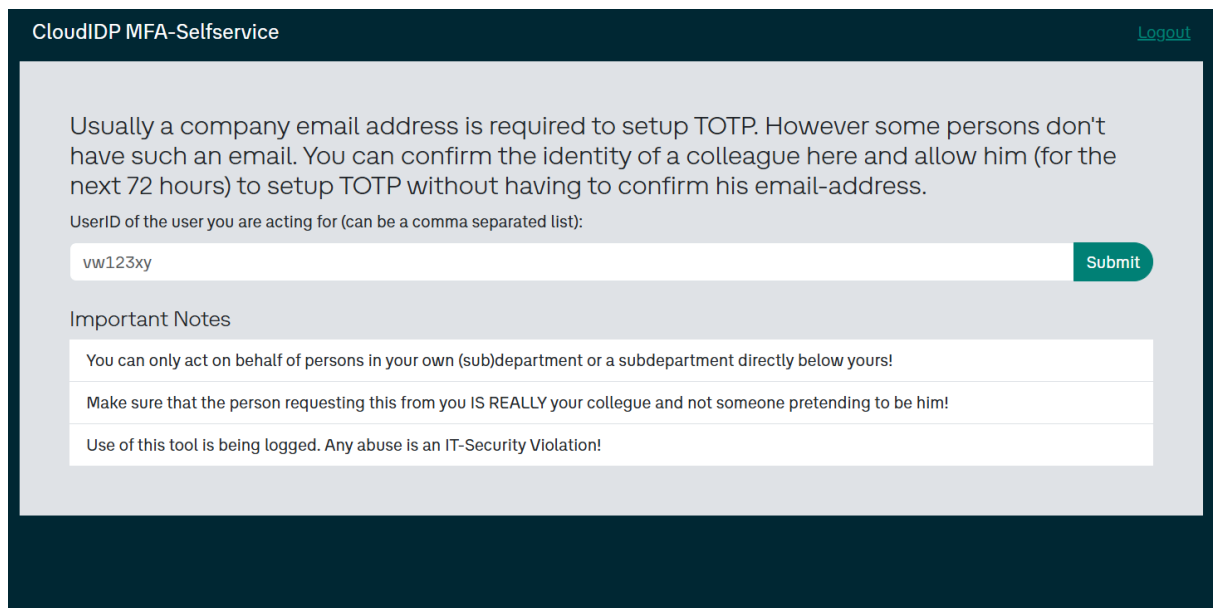
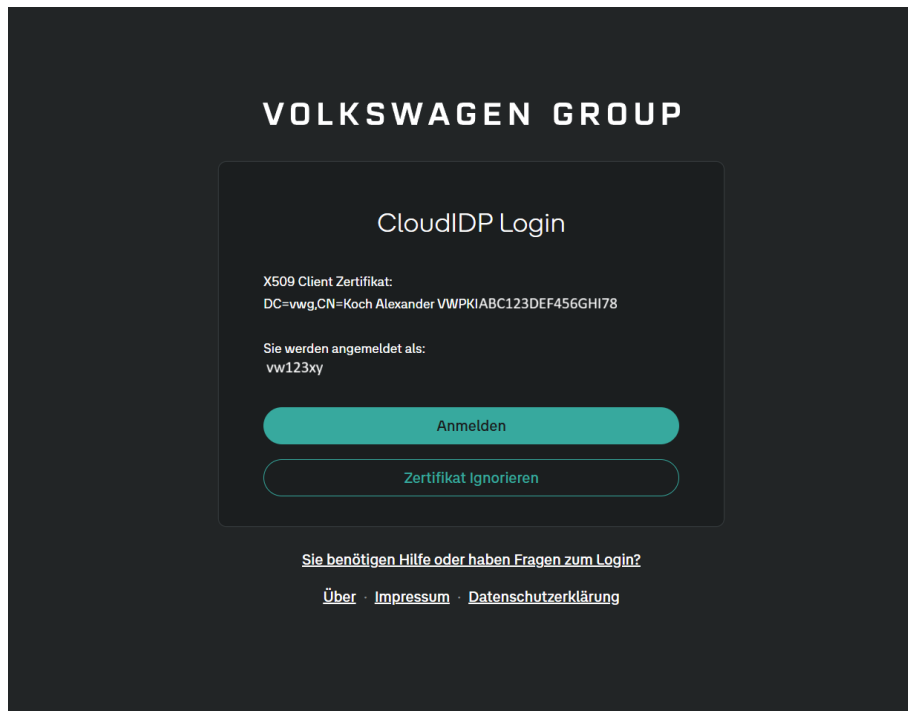
CloudIDP MFA-Selfservice

This site allows you to reset the TOTP-Credentials of your (direct) colleagues, in case they have lost it. Additionally you can allow a user who has no email-address to register for TOTP.

[Reset TOTP for a user*](#) [Allow TOTP-Setup without email*](#)

*A PKI-Card login is required to use this functionality

- Your colleague must then strongly authenticate with their PKI card and confirm your UserID in the following field.



- Once successful, a green confirmation box will appear, and you are authorized to start the TOTP registration process.

The screenshot shows a web interface titled "CloudIDP (qa) MFA-Selfservice" with a "Logout" link in the top right. The main content area contains the following text: "Usually a company email address is required to setup TOTP. However some persons don't have such an email. You can confirm the identity of a colleague here and allow him (for the next 72 hours) to setup TOTP without having to confirm his email-address." Below this is a label "UserID of the user you are acting for (can be a comma separated list):" and a text input field containing "vw123xy" with a "Submit" button to its right. A green confirmation box below the input field states: "The user vw4dktv can now (for the next 72h) register for TOTP without having to confirm his email-address!". Underneath is a section titled "Important Notes" with three bullet points: "You can only act on behalf of persons in your own (sub)department or a subdepartment directly below yours!", "Make sure that the person requesting this from you IS REALLY your colleague and not someone pretending to be him!", and "Use of this tool is being logged. Any abuse is an IT-Security Violation!".

- You now have 72 hours to complete the TOTP registration.
- **Register TOTP:** Visit the “Sign In” page of your CloudIDP account:
<https://idp.cloud.vwgroup.com/auth/realms/kums-mfa/account/account-security/signing-in>

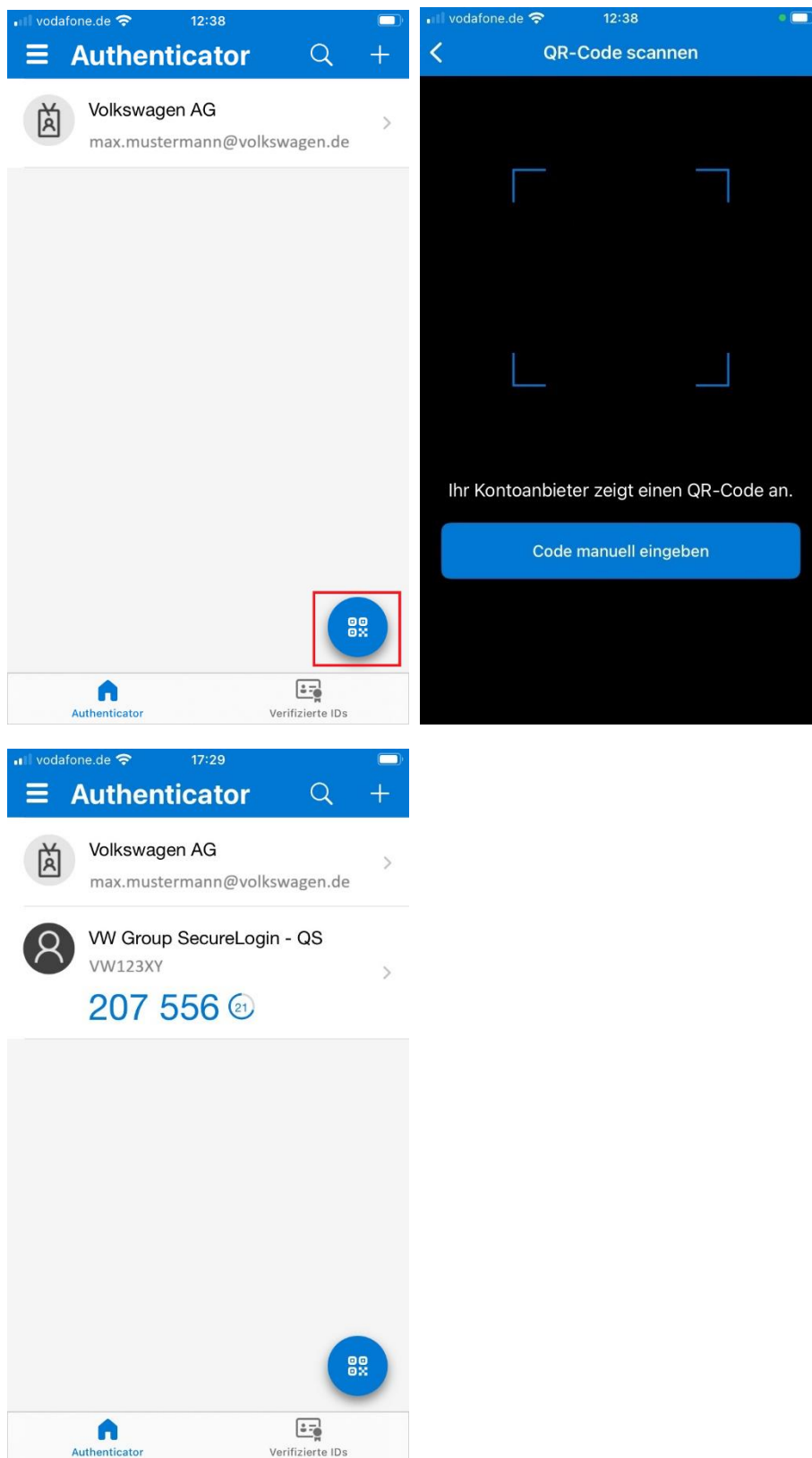
- Log in with your username and password.

The screenshot shows the 'Volkswagen Group CloudIDP Login' page. At the top, the 'Volkswagen Group' logo is displayed. Below it, the title 'CloudIDP Login' is centered. The form contains a 'Volkswagen Group User ID' field, a 'Password' field with a visibility toggle, and a 'Sign In' button. A link for 'Forgot password?' is provided. Below the main form is an 'Other Login-Method' button. A section titled 'Or sign in with' offers options for 'Microsoft Entra ID for Scania' and 'Group Secure Login'. At the bottom, there is a link for 'Need help or have questions about logging in?' and footer links for 'About', 'Imprint', and 'Privacy policy'.

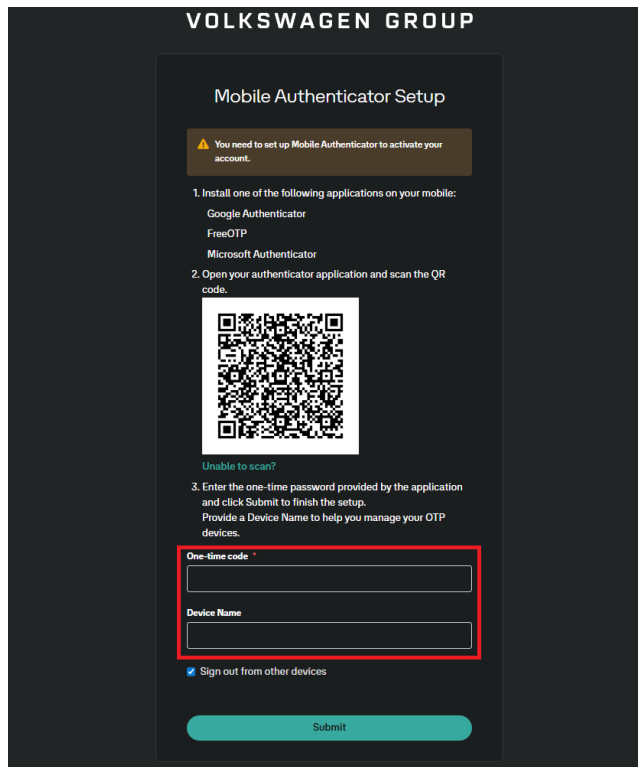
- After logging in, you must set up the authenticator app. Scan the QR code with an authenticator app of your choice (e.g., Microsoft Authenticator, Google Authenticator, Free OTP) on your private smartphone.

The screenshot shows the 'Volkswagen Group Mobile Authenticator Setup' page. It features a warning message: 'You need to set up Mobile Authenticator to activate your account.' The instructions are: 1. Install one of the following applications on your mobile: Google Authenticator, FreeOTP, or Microsoft Authenticator. 2. Open your authenticator application and scan the QR code. A QR code is displayed in the center. Below it is a link for 'Unable to scan?'. 3. Enter the one-time password provided by the application and click Submit to finish the setup. Provide a Device Name to help you manage your OTP devices. The form includes a 'One-time code' field, a 'Device Name' field, a checked checkbox for 'Sign out from other devices', and a 'Submit' button.

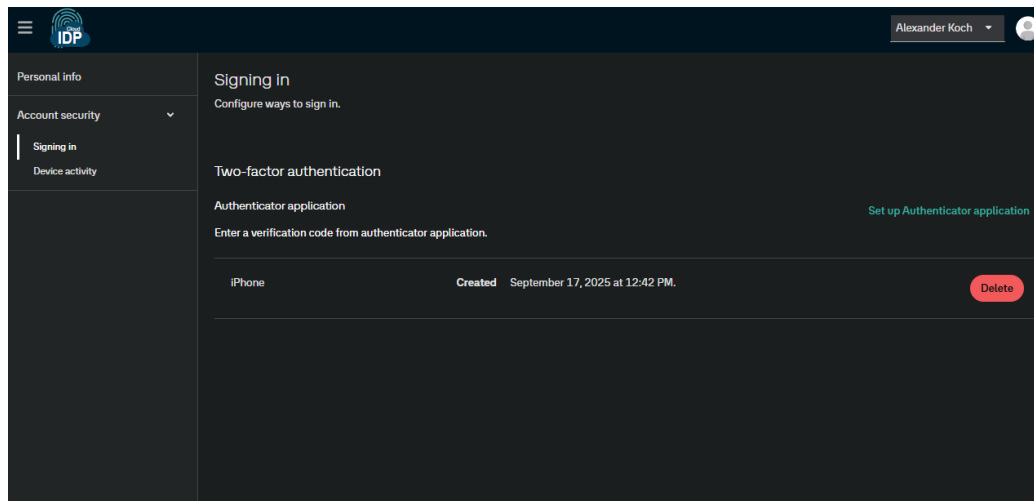
- Example with Microsoft Authenticator:



- Enter the one-time code from the app into the CloudIDP form. Optionally, enter a device name.



- Done! On the CloudIDP account page (<https://idp.cloud.vwgroup.com/auth/realms/kums-mfa/account/account-security/signing-in>), your registration status will now be displayed.

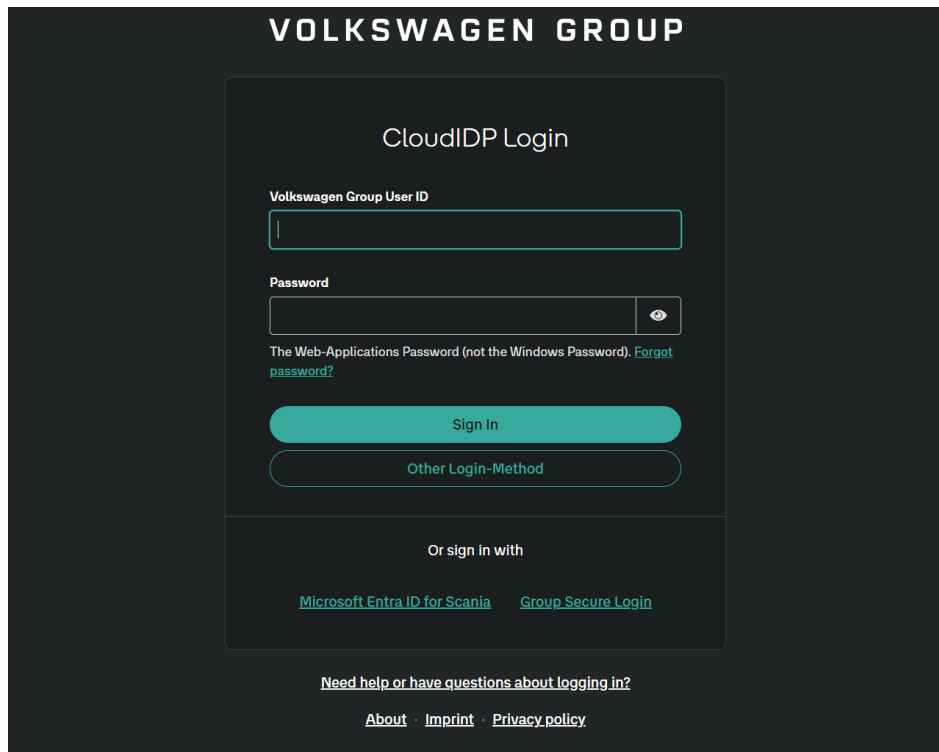


Note: In some companies, a central department is responsible for enabling TOTP setup without email, in case your direct supervisor does not have the required means.

TOTP authentication example

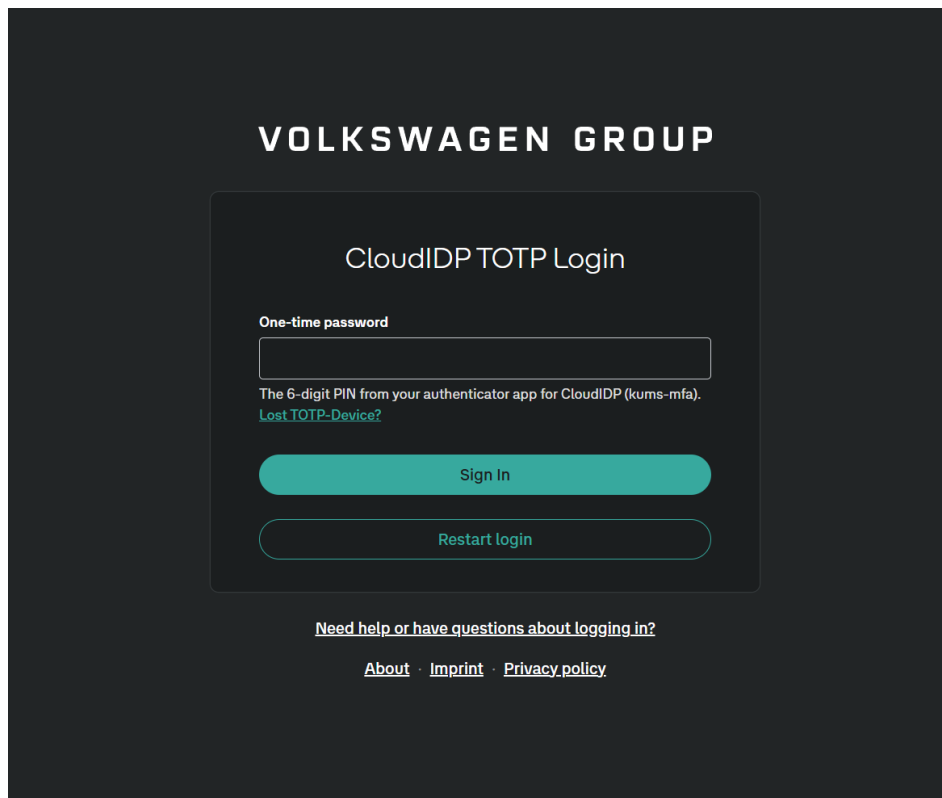
A typical login process with TOTP looks like this:

- The user enters their UserID + password.



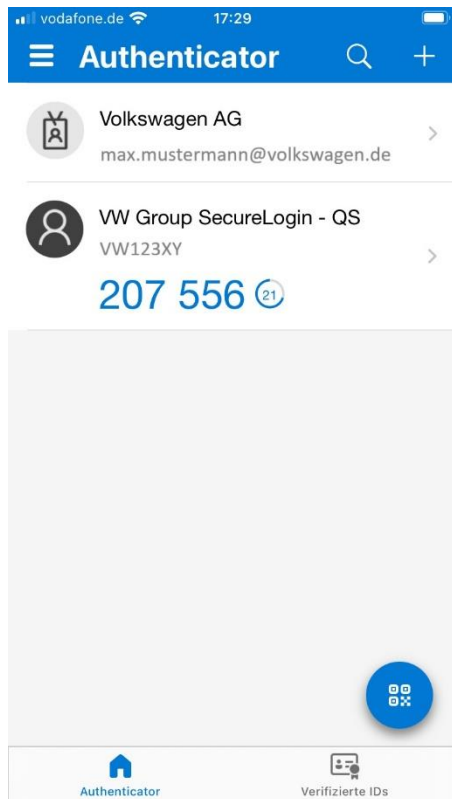
The screenshot shows the 'Volkswagen Group CloudIDP Login' page. It features a dark background with white text. At the top, the 'Volkswagen Group' logo is displayed. Below it, the title 'CloudIDP Login' is centered. The form includes two input fields: 'Volkswagen Group User ID' and 'Password'. The password field has a toggle icon for visibility. Below the password field, there is a note: 'The Web-Applications Password (not the Windows Password). [Forgot password?](#)'. There are two buttons: a teal 'Sign In' button and a white 'Other Login-Method' button. Below these, it says 'Or sign in with' followed by two links: '[Microsoft Entra ID for Scania](#)' and '[Group Secure Login](#)'. At the bottom, there is a link for 'Need help or have questions about logging in?' and footer links for 'About', 'Imprint', and 'Privacy policy'.

- In the next step, the one-time password from the authenticator app must be entered as the second factor.



The screenshot shows the 'Volkswagen Group CloudIDP TOTP Login' page. It features a dark background with white text. At the top, the 'Volkswagen Group' logo is displayed. Below it, the title 'CloudIDP TOTP Login' is centered. The form includes one input field: 'One-time password'. Below the input field, there is a note: 'The 6-digit PIN from your authenticator app for CloudIDP (kums-mfa). [Lost TOTP-Device?](#)'. There are two buttons: a teal 'Sign In' button and a white 'Restart login' button. At the bottom, there is a link for 'Need help or have questions about logging in?' and footer links for 'About', 'Imprint', and 'Privacy policy'.

- This 6-digit token appears in the app (e.g., Microsoft Authenticator). **Note:** Group Secure Login token are not support anymore for the login. (since 19.01.26)



Frequently Asked Questions (FAQ)

- **I have lost the TOTP secret. What to do?**

You have to start the registration process again. Your old secret (QR-code) will be invalid automatically.

- **Where will the One Time password be sent?**

To the mail address that is stored in K-LDAP.

You can check the mail address in VCD (<https://vcdweb.vw.vwg/>).

Validity of the mail: 5 minutes. Please also check the spam folder!

- **How can I edit/change the mail address in K-LDAP?**

Please use the processes of the “user & account management” (UAM, former KAM).

- **TOTP does not work despite the successful registration?**

Possibly the time of your phone is not in sync.

→ Activate automatic time synchronization on your phone.

→ If it does not help: Reset TOTP (with login via PKI card) at

<https://mfa.idp.cloud.vwgroup.com>

or with the support of a colleague of your department.

Alternative: You can create a support ticket via Help-Desk. The support can reset the registration so that you can register again.

- More Details on the registration process can be found in the internal Volkswagen

Wiki: [TOTP registration process - CloudIDP - Group Wiki](#)