

B2B introduction

- The main purpose of B2B Portal is to provide ŠKODA AUTO employees and their business partners (importers, dealers, etc.) important information and access to application of ŠKODA AUTO.

Get access

Security options

Login

Password reset

FAQ



ŠKODA

Get access

ŠKODA AUTO employee

Other B2B users

Please choose
one option and
click



ŠKODA

ŠKODA AUTO employee

For the first access:

- Open this URL: <https://Bportal.skoda.vwg>.
- Fill the reason.
- Choose Send request.
- Your request has been created , B2B team is going to contact you with the certificate.

The image displays two side-by-side screenshots of the ŠKODA B2B Portal interface. Both screenshots show the 'SIMPLY CLEVER' header and the ŠKODA logo. The left screenshot shows the 'Bez oprávnění' (No authorization) message and the 'Nemáte potřebná práva pro práci s B2B Portálem.' (You do not have the necessary rights for working with the B2B Portal.) message. Below this, there is a text input field for 'Zdůvodnění' (Justification) and a 'Odeslat žádost' (Send request) button. The right screenshot shows the 'Bez oprávnění' (No authorization) message and the 'Nemáte potřebná práva pro práci s B2B Portálem.' (You do not have the necessary rights for working with the B2B Portal.) message. Below this, there is a confirmation message: 'Žádost čílo 301 024 byla odeslána' (Request number 301 024 has been sent).

Continue



ŠKODA

ŠKODA AUTO employee

- After receiving the certificate and a password from B2B team to you e-mail, please install the certificate according [this manual](#).
- During the first login it is necessary to set a new password.

Password rules

- The password cannot be identical to your user name.
- The password must be a combination of letters and at least one special character.
- The system remembers the last 6 passwords – those passwords cannot be used as a new password.
- The validity of password is 90 days.



Other B2B users

- For the first access to B2B Portal, please contact your OrgAdmin and he will create an electronic request.
- Backup solution is [this paper form](#) (filled send to address: b2bhelp@skoda-auto.cz).
- After receiving the certificate to your e-mail and installation password from your OrgAdmin, please install your certificate according to [this manual](#).
- After installation of your certificate, during the first login it is necessary to set a new password.

Password rules

- The password cannot be identical to your user name.
- The password must be a combination of letters and at least one special character.
- The system remembers the last 6 passwords – those passwords cannot be used as a new password.

*extra for users from Poland

- Every password must be a combination of at least one lowercase and uppercase letter, number and a special character.
- The validity of password is 30 days.

PASSWORD CHANGE

New password:

Password confirmation:



Login

Basic

Two-factor



Basic login

User name + password

Certificate + password

Other login methods



Two-factor login

User name + password + One-time password from SMS

User name + password + One-time password from Authenticator

User name + Tokencode

PKI (Employee ID card) + PIN

Only for
ŠKODA AUTO
employees




ŠKODA

User name + password

Login instructions:

1. Enter the required URL.
2. Enter:
 - User name.
 - Password.
3. You are logged in.



LOGIN

[Forgot password?](#)

CONTINUE

[Other login methods](#)

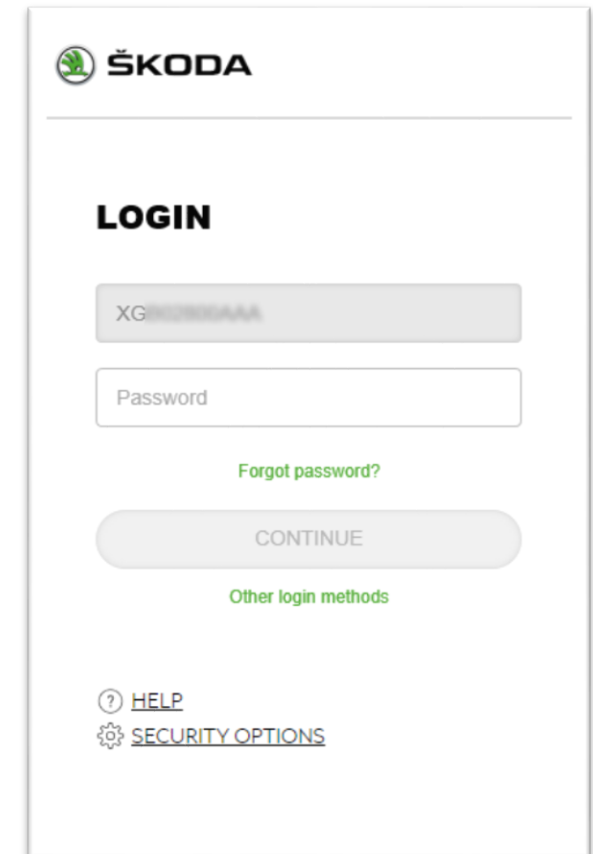
[? HELP](#)

[⚙ SECURITY OPTIONS](#)

Certificate CA Partner + password

Login instructions:

1. Enter the required URL.
2. The available certificates are displayed in the browser. Choose the appropriate one.
3. Enter:
 - Password.
4. You are logged in.



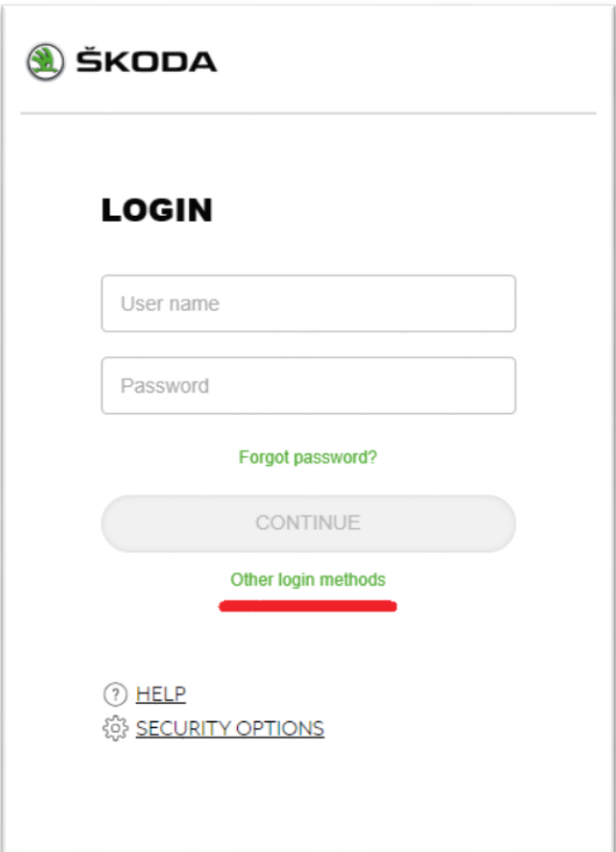
The screenshot shows the ŠKODA login interface. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is displayed in bold. There are two input fields: the first contains "XG" followed by masked characters, and the second is labeled "Password". Below the password field is a green link "Forgot password?". A large, rounded "CONTINUE" button is centered below the links. At the bottom, there are two links: "? HELP" and a gear icon followed by "SECURITY OPTIONS".

Other login methods

- Link is available in the „Basic login“ screen only.
- User can use higher authentication levels after clicking the link „Other login methods“.

Login instructions:

1. Enter the required URL.
2. Click „Other login methods“.
3. Based on chosen method, follow instructions for [SMS](#), [Authenticator](#), [RSA Tokencode](#).




The screenshot displays the ŠKODA login page. At the top left is the ŠKODA logo. Below it, the word "LOGIN" is centered. There are two input fields: "User name" and "Password". Below the "Password" field is a green link "Forgot password?". A grey "CONTINUE" button is positioned below the "Forgot password?" link. Below the "CONTINUE" button is a green link "Other login methods" which is underlined with a red line. At the bottom left, there are two links: "HELP" (with a question mark icon) and "SECURITY OPTIONS" (with a gear icon).

User name + password + One-time password from SMS

First it is necessary to registrate the device.

Login instructions:




1. Enter the required URL.
2. Choose method of authentication via SMS and confirm.
3. Enter:
 - User name.
 - Password.



LOGIN


Step 1 / 3

Select verification methods

 SMS  Authenticator  RSA

CONTINUE

[? HELP](#)
[SECURITY OPTIONS](#)



LOGIN

Step 2 / 3

[Forgot password?](#)

CONTINUE

[BACK](#)

[? HELP](#)
[SECURITY OPTIONS](#)

Continue

User name + password + One-time password from SMS


4. This step is skipped based on following rules:

In case user has got more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and confirms the form.

In case user has got only one device registered and activated, the device is chosen automatically and user is redirected to step 5 directly.

5. Enter the code from SMS.

6. You are logged in.



LOGIN

Step 3 / 3

Select device


☐ TEST 1 (+44123456789)

☐ TEST 2 (+44987744522211)

SMS with authentication code will be send to the chosen phone.

SEND SMS

BACK



LOGIN

Step 3 / 3

Selected device

☒ TEST 2 (+44987744522211)

Copy the code in SMS.

Verifying code

VERIFY

RESEND SMS

BACK

User name + password + One-time password from Authenticator

First it is necessary to registrate.

Login instructions:

1. Enter the required URL.
2. Choose method of authentication via Authenticator and confirm.
3. Enter:
 - User name.
 - Password.

The image displays two sequential screenshots of the ŠKODA login interface. Both screens feature the ŠKODA logo at the top left.

Left Screenshot (Step 1 / 3): The title is "LOGIN". Below it, the text "Step 1 / 3" and "Select verification methods" are shown. There are two options: "Authenticator" (represented by a green QR code icon) and "RSA" (represented by a green key icon). A large, light gray "CONTINUE" button is centered below these options. At the bottom, there are links for "? HELP" and a gear icon followed by "SECURITY OPTIONS".

Right Screenshot (Step 2 / 3): The title is "LOGIN". Below it, the text "Step 2 / 3" is shown. There are two input fields: "User name" and "Password". Below the "Password" field is a green link "Forgot password?". A large, light gray "CONTINUE" button is centered below these fields. Below the "CONTINUE" button is a link "BACK". At the bottom, there are links for "? HELP" and a gear icon followed by "SECURITY OPTIONS".

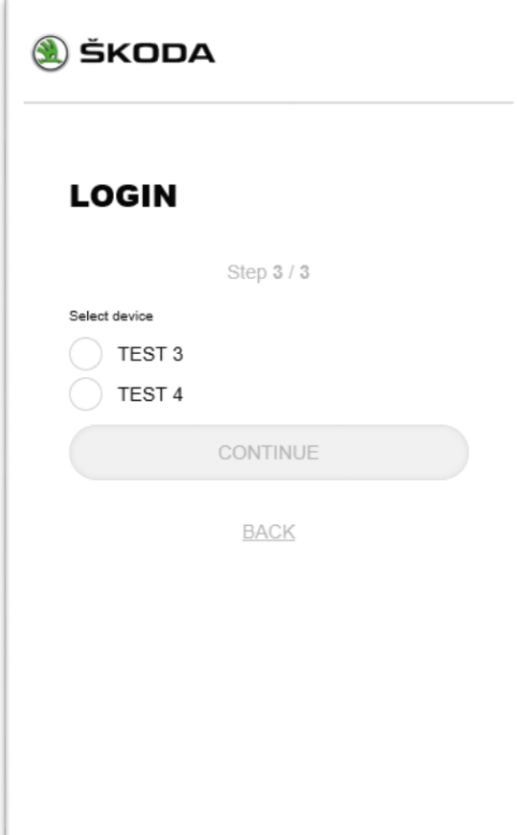
Continue

User name + password + One-time password from Authenticator

4. This step is skipped based on following rules:

In case user has got more devices registered and activated, the list of all active devices is displayed. User chooses one of the devices and confirms the form.

In case user has got only one device registered and activated, the device is chosen automatically and user is redirected to step 5 directly.



ŠKODA

LOGIN

Step 3 / 3

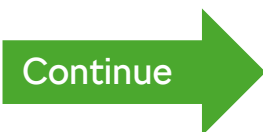
Select device

☐ TEST 3

☐ TEST 4

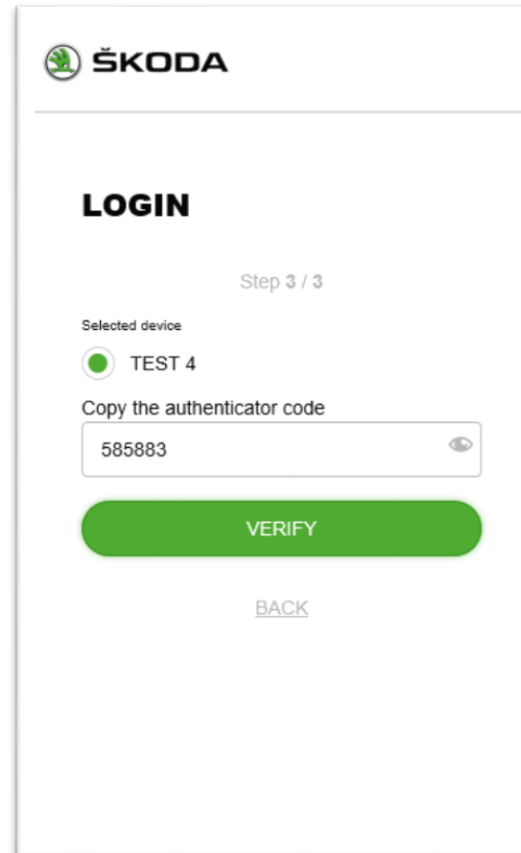
CONTINUE

[BACK](#)

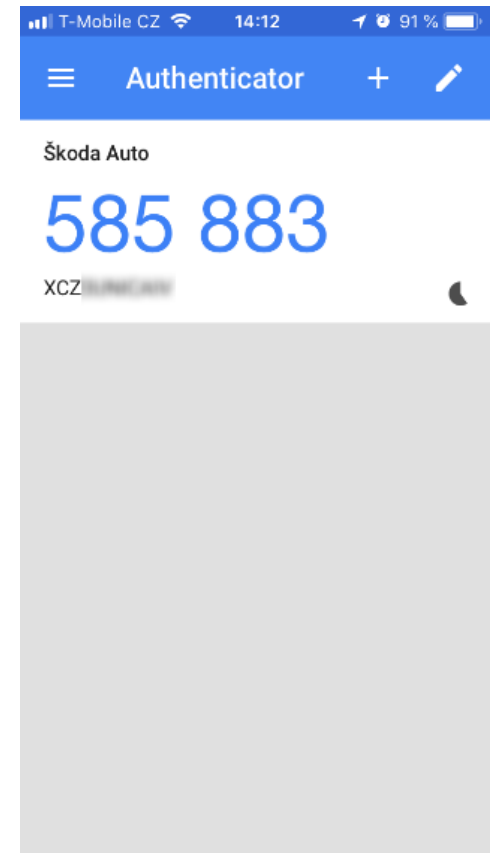


User name + password + One-time password from Authenticator

5. You are prompted for one-time password entry from Authenticator (on your mobile device) and confirm.
6. You are logged in.



The screenshot shows the ŠKODA LOGIN interface. At the top is the ŠKODA logo. Below it, the word "LOGIN" is displayed. The progress indicator shows "Step 3 / 3". Under "Selected device", "TEST 4" is selected with a green circle. The prompt "Copy the authenticator code" is followed by a text input field containing "585883" and a toggle icon. A large green "VERIFY" button is below the input field, and a "BACK" link is at the bottom.



User name + Tokencode

Login instructions:

1. Enter the required URL.
2. Enter:
 - User name.
 - PIN + Tokencode.
3. Choose method of authentication RSA and confirm.
4. You are logged in.

The image displays two sequential screenshots of the ŠKODA login interface.

Left Screenshot (Step 1/2):

- Header: ŠKODA logo.
- Title: LOGIN
- Step indicator: Step 1 / 2
- Instruction: Select verification methods
- Option: RSA (indicated by a green toggle switch)
- Button: CONTINUE
- Footer: [? HELP](#) and [SECURITY OPTIONS](#)

Right Screenshot (Step 2/2):

- Header: ŠKODA logo.
- Title: LOGIN
- Step indicator: Step 2 / 2
- Input fields: User name and RSA Tokencode
- Button: CONTINUE
- Link: [BACK](#)
- Footer: [? HELP](#) and [SECURITY OPTIONS](#)

PKI (Employee ID card) + PIN

Login instructions:

1. Enter the required URL.
2. A certificate (from PKI card) selection window appears. Choose the corresponding one.
3. You are logged in and redirected to required URL.



Security options

Registration

Activation



ŠKODA

Registration


Click "Security options" for adding new device.

1. Click the link "Security options" - new tab will be opened.

2. Enter:

- User name.
- Password.

3. You are logged in.



LOGIN


[Forgot password?](#)

CONTINUE

[Other login methods](#)

[? HELP](#)

[? SECURITY OPTIONS](#)



LOGIN

[Forgot password?](#)

CONTINUE

[? HELP](#)

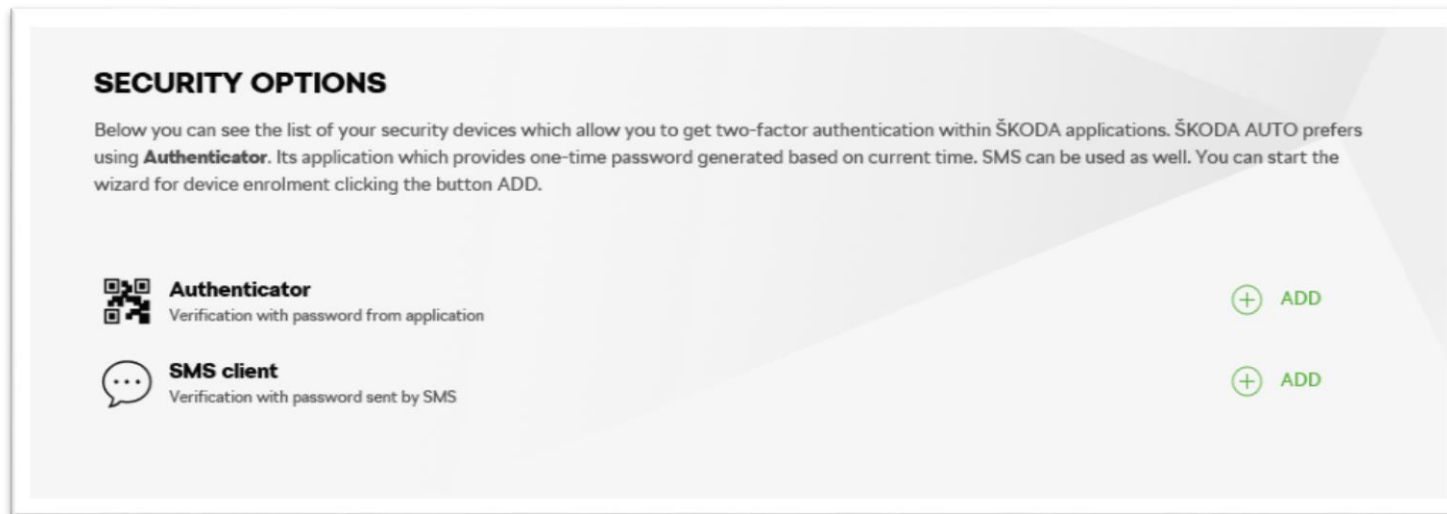


Registration

- Use the ADD button to select the device you want to register.
- It's possible to have more authentication devices. You can also delete the device.

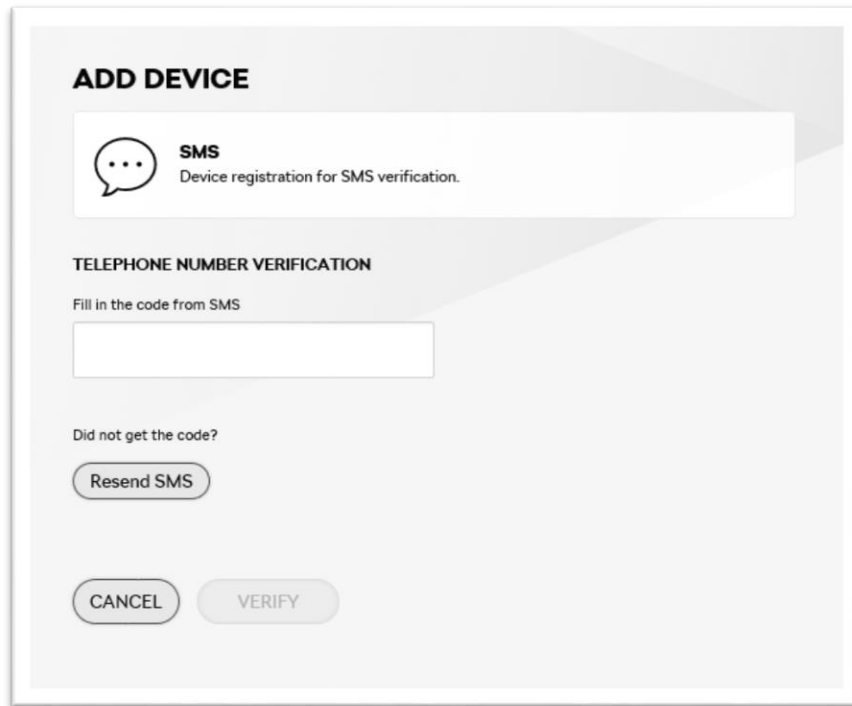
SMS

Authenticator




SMS

- Enter:
 - Name of your device.
 - Telephone number, preselection.



ADD DEVICE

 **SMS**
Device registration for SMS verification.

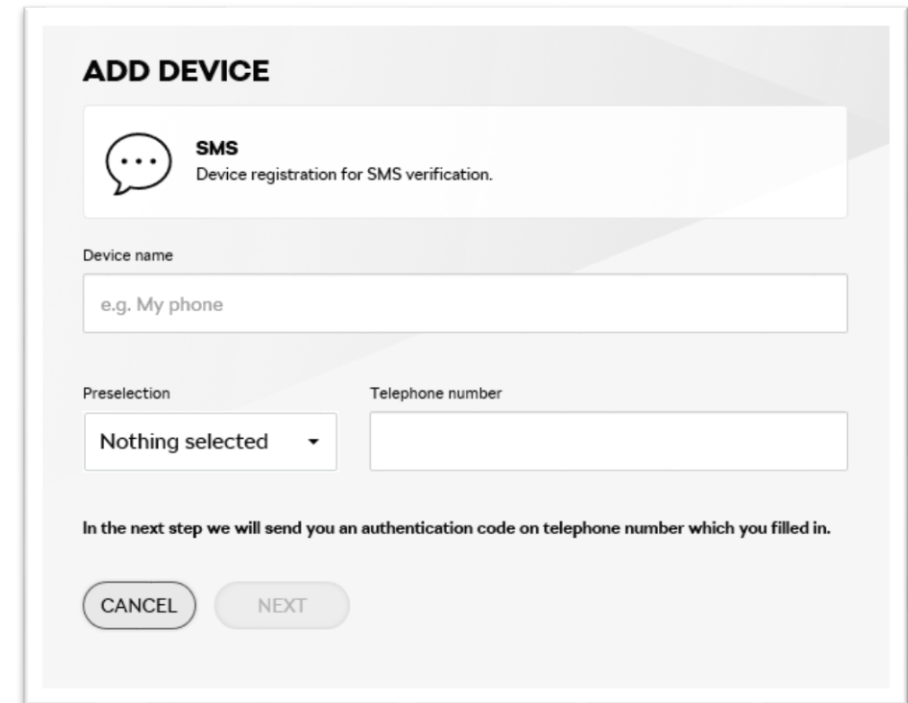
TELEPHONE NUMBER VERIFICATION

Fill in the code from SMS


Did not get the code?

[Resend SMS](#)

[CANCEL](#) [VERIFY](#)



ADD DEVICE

 **SMS**
Device registration for SMS verification.

Device name

Preselection Telephone number

[Nothing selected](#)

In the next step we will send you an authentication code on telephone number which you filled in.

[CANCEL](#) [NEXT](#)

- The user is asked to enter the code from to SMS and confirms it.

Activation

Authenticator

**Authenticator – web
browser application**


**Authenticator – mobile
application**



Authenticator registration

- Enter:
 - Name of your device.


ADD DEVICE

 **Authenticator**
Device registration for authentication with application

1. Install application FreeOTP - [Android/iOS](#), or Google Authenticator - [Android/iOS](#).

2. With application scan QR code. If you are unable to scan the QR code, fill in the secret key manually. Make sure your screen is not tracked by anyone - sensitive information will be displayed.


[Hide QR code](#) (27)





Secret key
FF6M5Z7FN2ZA542INTRL366T5TRDOH4Q

Link for authenticator configuration
[Add authenticator](#)


Fill in the code from application.

 **ŠKODA** Auth

User
Name Surname

ADD DEVICE

 **Authenticator**
Device registration for authentication with application

Device name

- 2.Click “Show the QR code” and copy the “Secret key”. Keep the window opened. Next step is to install the browser addon. Follow „Firefox addon installation guide“.

Continue

Firefox addon installation guide

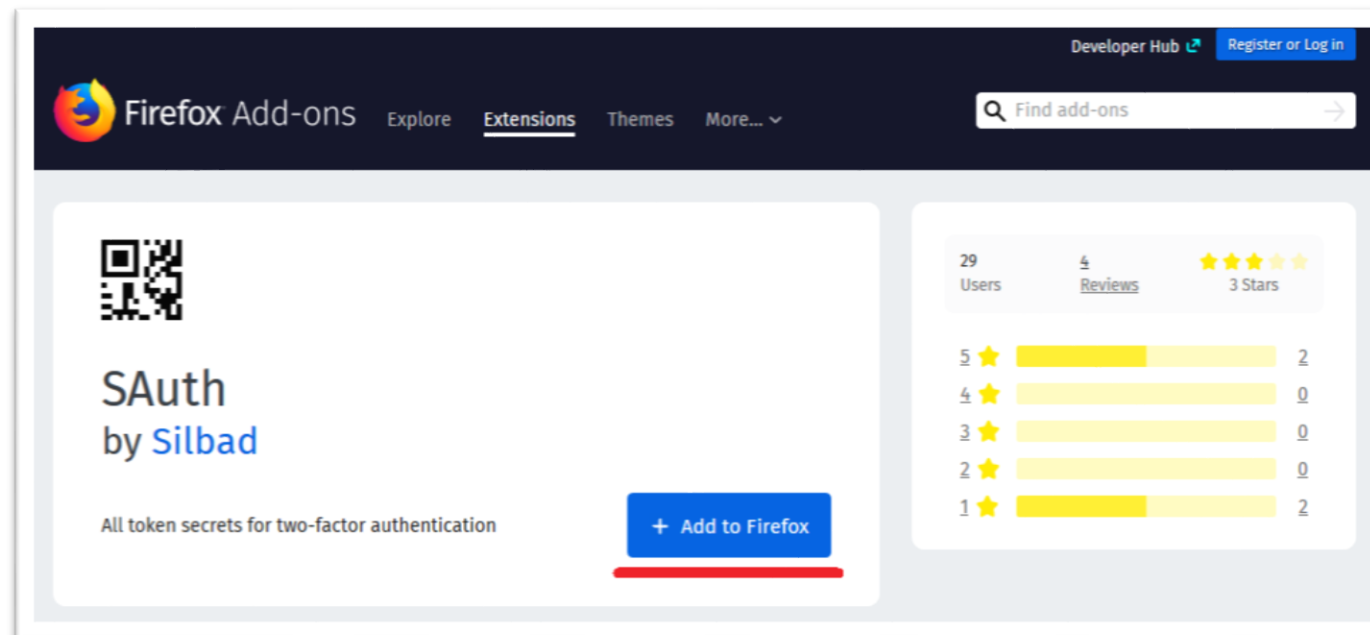
This help contains guide for installation the addon SAuth for Firefox („FF“). There are other possibilities for other browsers as well. For example for Internet Explorer, Google Chrome. Such instruction is not a part of this help and can differ.

Attention: The guide is based on 3rd party application. We reserve the right to make changes.

If you don't have got the FF installed, follow this link: <https://www.mozilla.org/firefox/new/>

3.Open following URL in Firefox - <https://addons.mozilla.org/firefox/addon/sauth/>

4.Click the button “Add to Firefox”.



5.Accept the confirmation dialogue. Click “Add”.

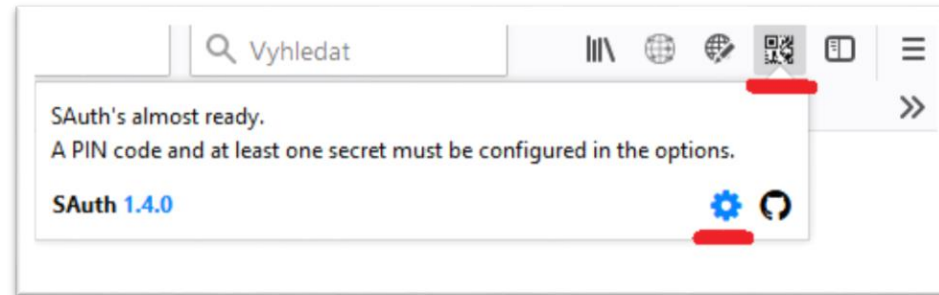
Continue



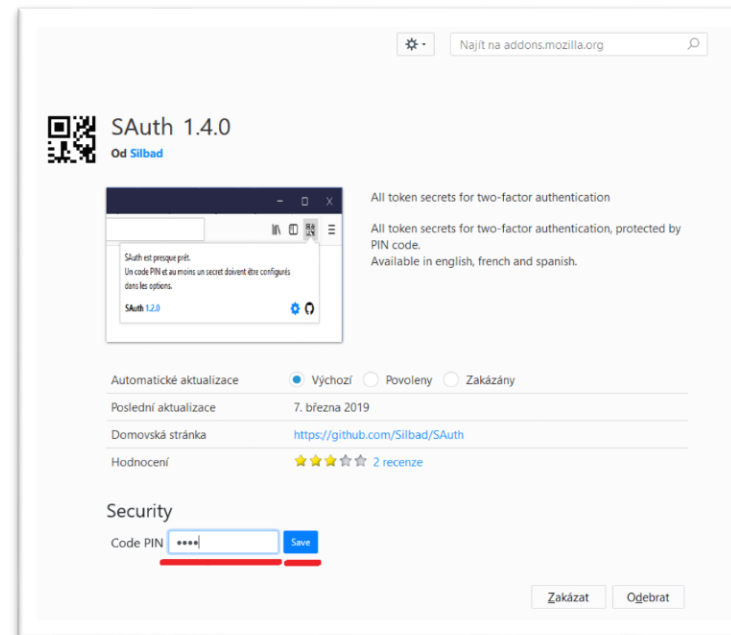
ŠKODA

Firefox addon installation guide

6. Launch the Sauth application.



7. Enter PIN and click “Save”.





Firefox addon installation guide

8.In “Secrets list” enter parameters:

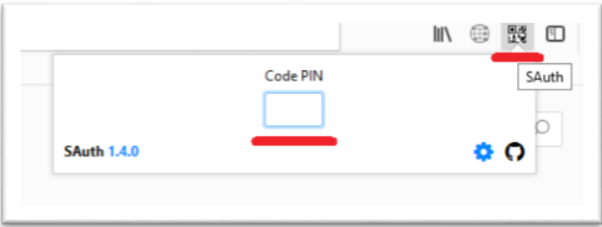
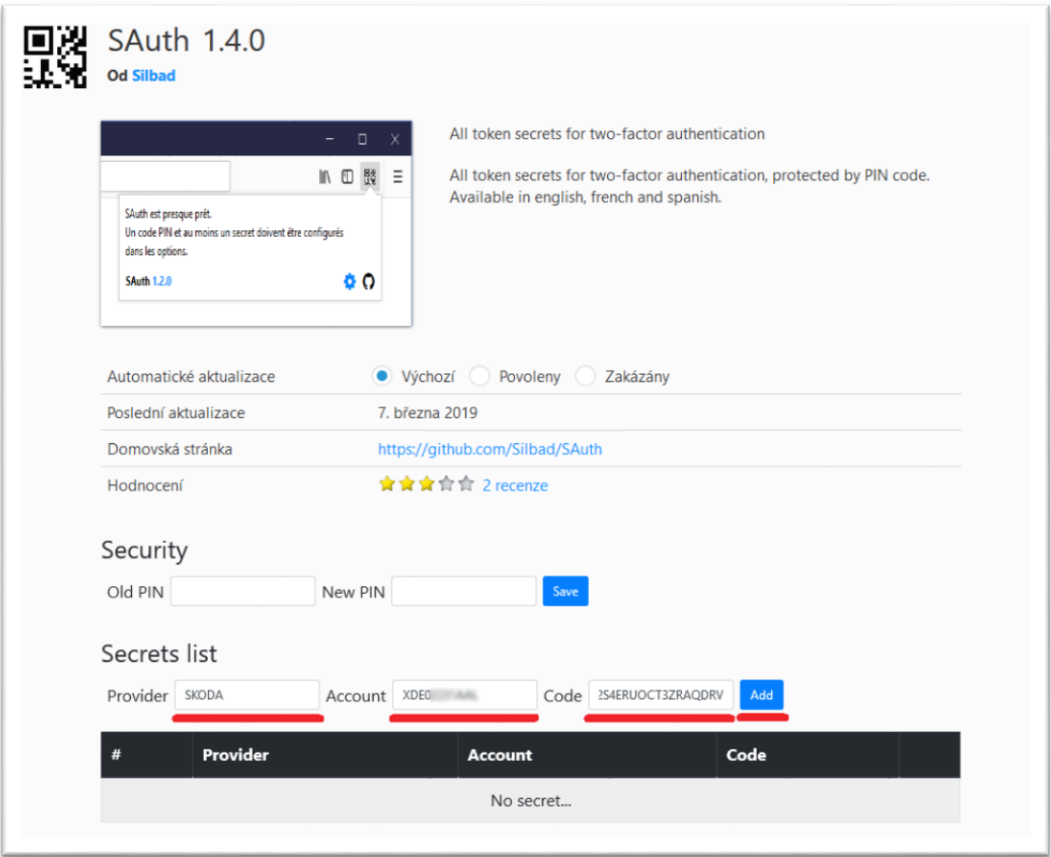
- Provider – SKODA.
- Account – Any value, f.e. your User name
- Code – Insert the “Secret key” from the device registration (Security options).

Click the button „Add“.

9.The device is succesfully added to the application and it's ready to use. You can close the window.

| # | Provider | Account | Code | |
|---|----------|--------------|-------|---|
| 1 | SKODA | XDE00771AAAL | ***** |   |

10.Open the SAuth application in the browser and unlock it using the PIN which was established.

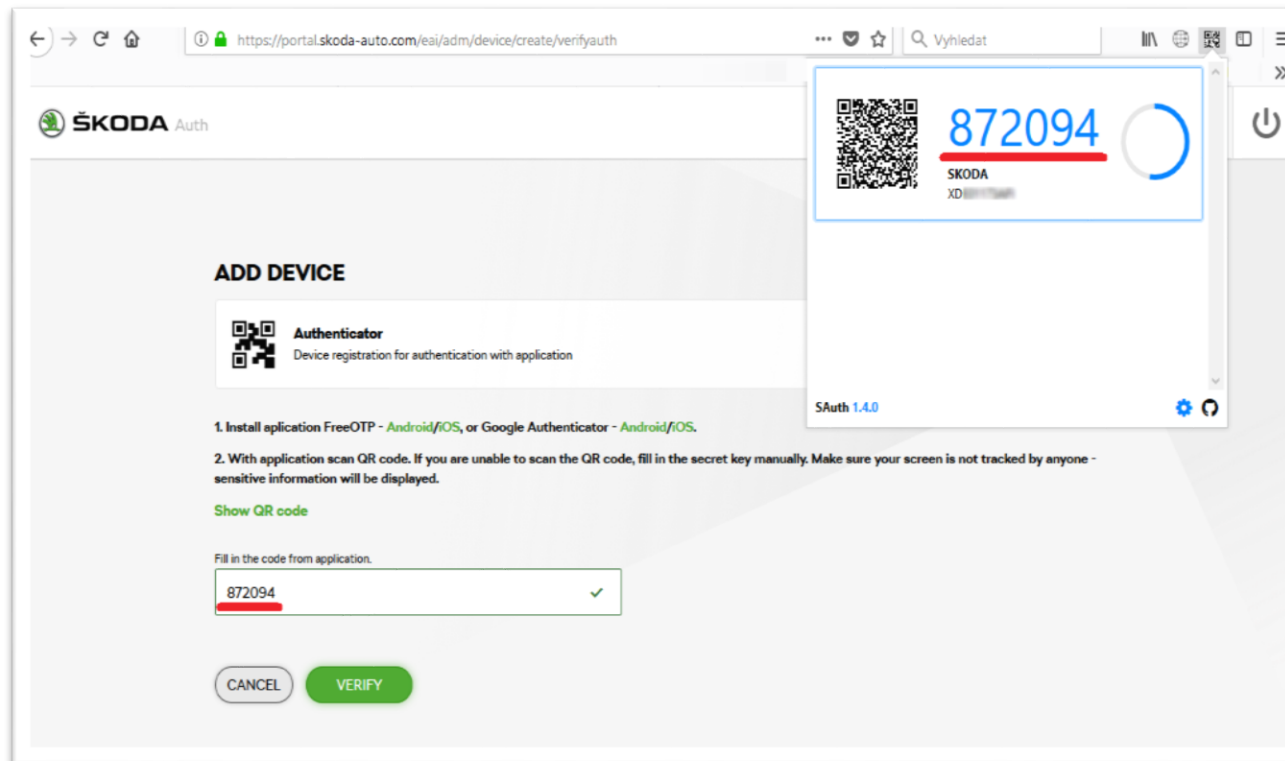


Firefox addon installation guide

Go back to the Security Options:

11. Re-type the generated code to the SECURITY OPTIONS. (It could be done within 30 seconds).

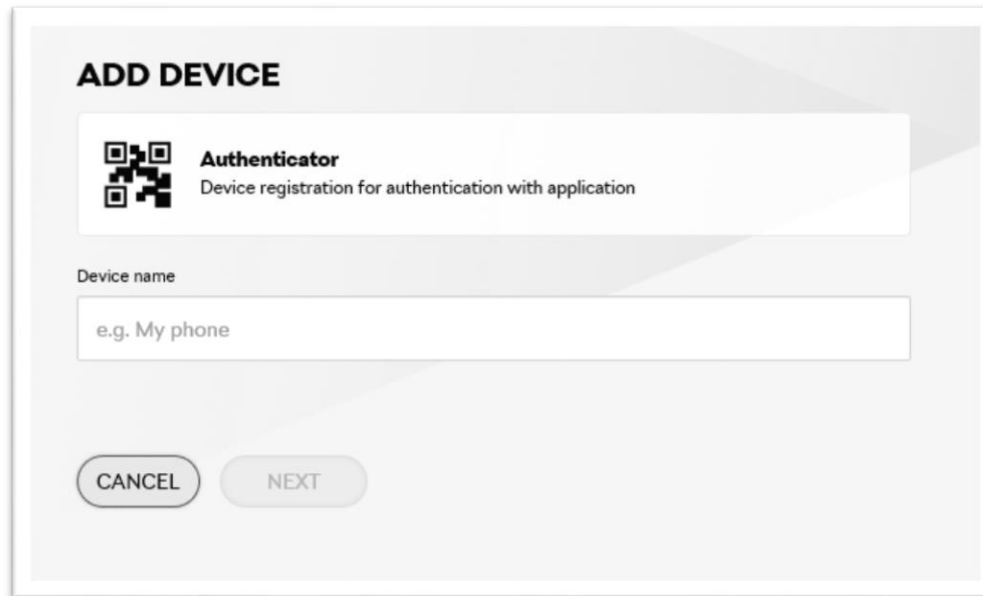
12. Click the button “Verify”, the device is created.



Activation

Authenticator registration

- Enter:
 - Name of your device.



The image shows a dialog box titled "ADD DEVICE". Inside the dialog, there is a section with a QR code icon and the text "Authenticator" followed by "Device registration for authentication with application". Below this, there is a label "Device name" and a text input field containing the placeholder text "e.g. My phone". At the bottom of the dialog, there are two buttons: "CANCEL" and "NEXT".

- Keep the window opened. Next step is to install the mobile application (f.e. FreeOTP / Google Authenticator).

Continue



ŠKODA


Authenticator registration

Go back to the Security Options:

2. Click Show the QR code and read it using the mobile application

3. Retype the 6 characters code from mobile app to the Security Options to appropriate field. The code expires after 30 seconds.

ADD DEVICE

**Authenticator**
Device registration for authentication with application

1. Install application FreeOTP - [Android/iOS](#), or Google Authenticator - [Android/iOS](#).

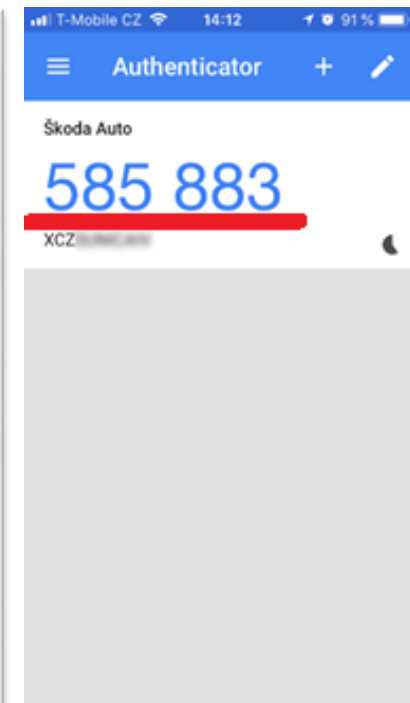
2. With application scan QR code. If you are unable to scan the QR code, fill in the secret key manually. Make sure your screen is not tracked by anyone - sensitive information will be displayed.

[Show QR code](#)

Fill in the code from application.

✓

CANCELVERIFY



Activation



ŠKODA

Activation

ŠKODA AUTO employee

Other B2B users



ŠKODA

Device activation for ŠKODA AUTO employee

- List of available activation methods is displayed:
 - Activation using two-factor authentication
 - Activation using Print2me
- User chooses the wanted method by clicking the appropriate button Continue

The screenshot shows a web interface for device activation. At the top, a blue banner contains the following text: "Authenticator verification was successful. For activation select one of the available methods. Without activation the device will be automatically deleted in 720 days. The activation code for Print2me was sent to the printer. You can withdraw it using your employee ID card." Below this banner is the section "ADD DEVICE". It contains three options: 1. "SMS" with a speech bubble icon and the text "Device registration for SMS verification." 2. "Activate using two-factor authentication" with a blue "Continue" button. The text below it says: "Activation can be done using two-factor authentication. While you login via RSA Tokencode or employee card (PKI) to reach two-factor authentication level, the device will be activated." 3. "Activate using Print2me" with a blue "Continue" button. The text below it says: "Print2me is service which offers printing based on employee ID card authentication. You can send activation codes using the Print2me service and withdraw the activation code by printing at the nearest printer. Once you have the activation code, you can use this method for activation. After the activation code is inserted, the device is activated." At the bottom left of the form is a "CANCEL" button.

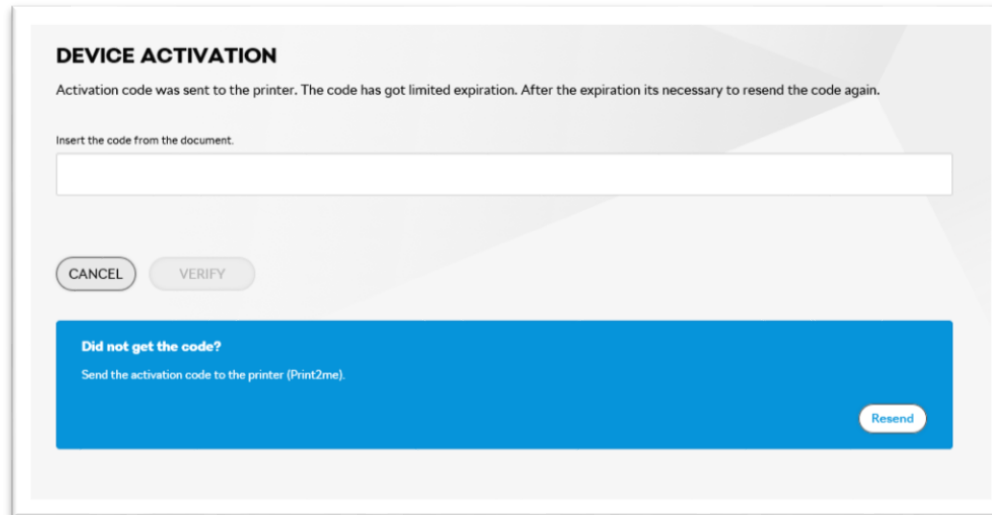
Continue



ŠKODA

Device activation for ŠKODA AUTO employee

- [Activation using Print2me](#)
- The code is sent to the printer, where user can print it using employee card.
- User enters the code from document and confirms.
- The device is activated.

A screenshot of a web interface for device activation. The title is "DEVICE ACTIVATION". Below it, a message states: "Activation code was sent to the printer. The code has got limited expiration. After the expiration its necessary to resend the code again." There is a text input field with the placeholder "Insert the code from the document." Below the input field are two buttons: "CANCEL" and "VERIFY". At the bottom, there is a blue box with the text "Did not get the code?" and "Send the activation code to the printer (Print2me)." with a "Resend" button.

- [Activation using two-factor authentication](#)
- User is redirected to Login page where are two-factor methods available - [SMS](#), [Authenticator](#), [RSA](#).
- Once user is logged in the device is activated within Security options.

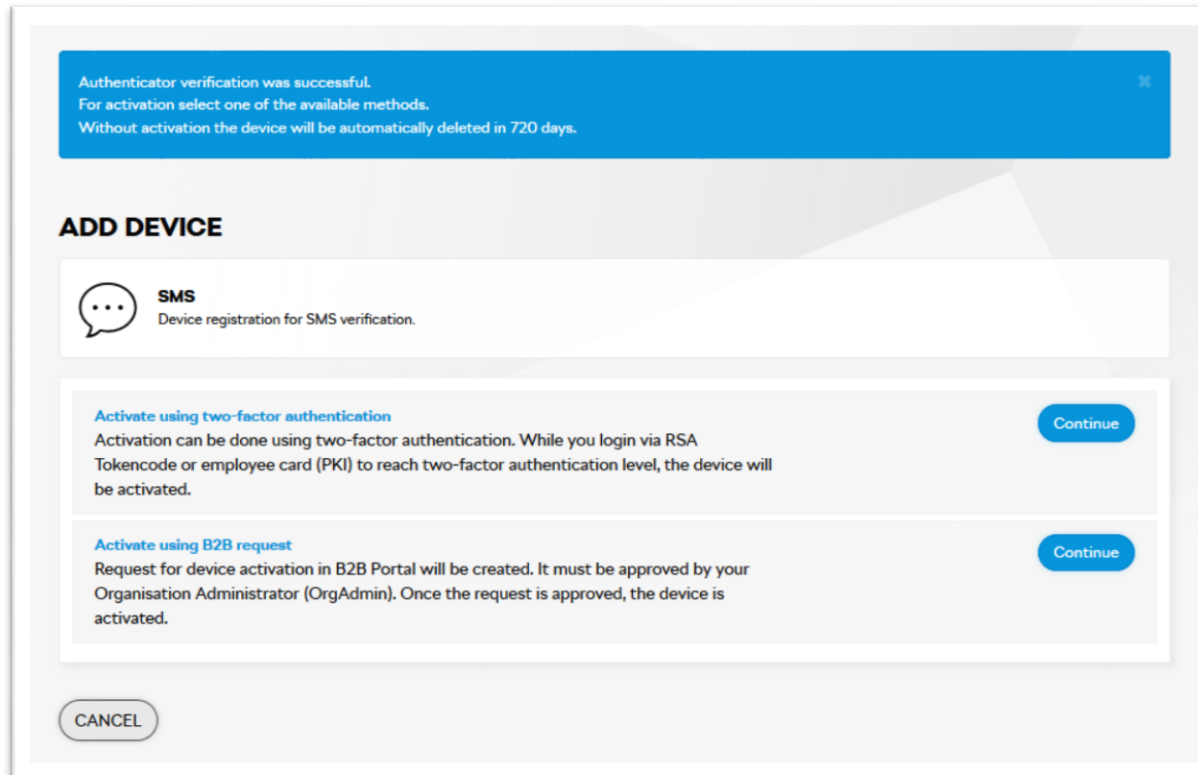
Login



ŠKODA


Device activation for other B2B users

- List of available activation methods is displayed:
 - Activation using two-factor authentication
 - Activation using B2B request
- User chooses the wanted method by clicking the appropriate button Continue



Authenticator verification was successful.
For activation select one of the available methods.
Without activation the device will be automatically deleted in 720 days.

ADD DEVICE

 **SMS**
Device registration for SMS verification.

[Activate using two-factor authentication](#) [Continue](#)
Activation can be done using two-factor authentication. While you login via RSA Tokencode or employee card (PKI) to reach two-factor authentication level, the device will be activated.

[Activate using B2B request](#) [Continue](#)
Request for device activation in B2B Portal will be created. It must be approved by your Organisation Administrator (OrgAdmin). Once the request is approved, the device is activated.

[CANCEL](#)

Continue



ŠKODA

Device activation for other B2B users

- Activation using B2B request
 - User is redirected to the initial page within “Security Options”
 - The request is automatically created and sent to the B2B Portal application.
 - Request approver is user’s Organization Administrator.
 - Once the request is approved, the device is activated and the user is notified by e-mail
- Activation using two-factor authentication
 - User is redirected to Login page where are two-factor methods available - SMS, Authenticator, RSA.
 - Once user is logged in the device is activated within Security Options.

Login



ŠKODA

Password reset

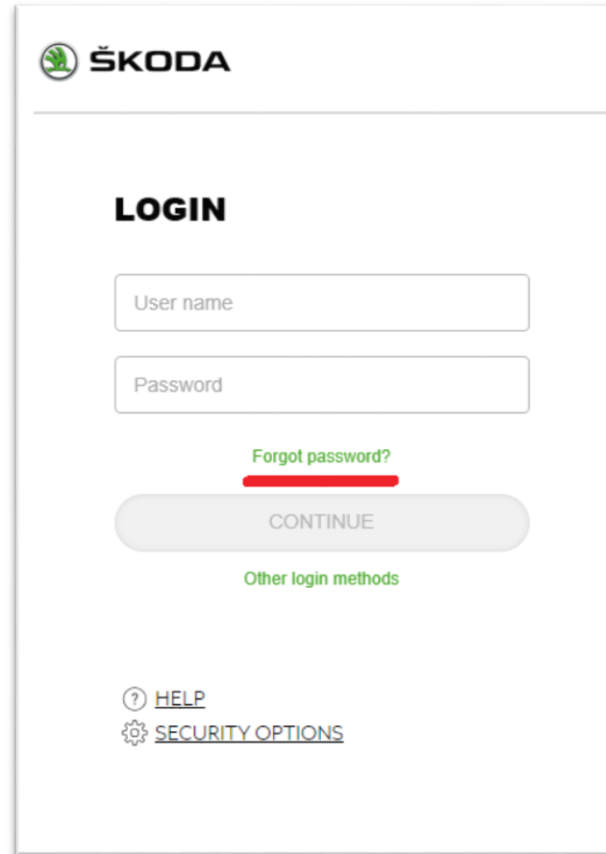
- It is possible to reset your password on login page of B2B Portal.
- The link „Forgot password“ is available in the „Basic login“ screen and as well from second step of SMS and Authenticator login method.

Instructions:

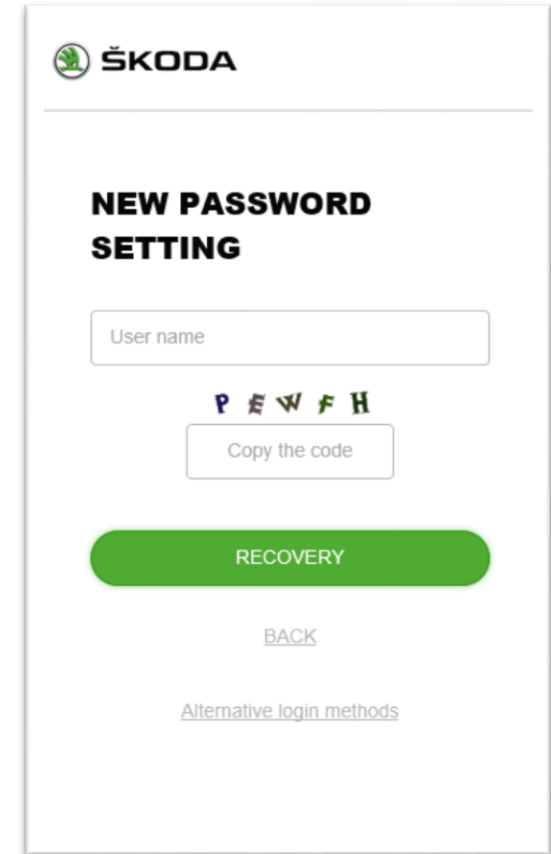
1. Click the link „Forgot password?“
2. User enters and confirms:

- User name
- Re-captcha security code

User can use the method which does not require the password using the link „Alternative login methods“. The process is described in appropriate chapter [here](#).



The screenshot shows the 'LOGIN' page of the ŠKODA B2B Portal. At the top is the ŠKODA logo. Below it, the title 'LOGIN' is centered. There are two input fields: 'User name' and 'Password'. Below the 'Password' field is a link 'Forgot password?' with a red underline. A large grey button labeled 'CONTINUE' is centered below the link. Below the button is a link 'Other login methods'. At the bottom, there are two links: 'HELP' with a question mark icon and 'SECURITY OPTIONS' with a gear icon.

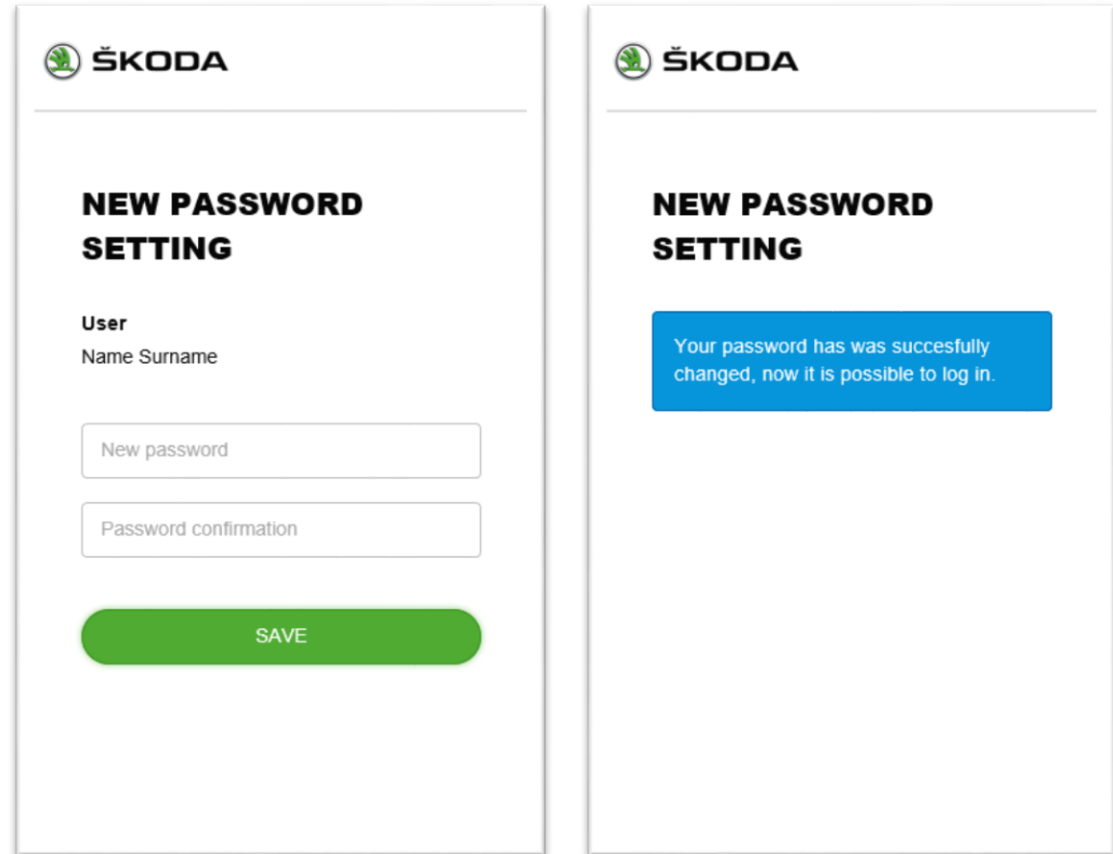



The screenshot shows the 'NEW PASSWORD SETTING' page of the ŠKODA B2B Portal. At the top is the ŠKODA logo. Below it, the title 'NEW PASSWORD SETTING' is centered. There is one input field: 'User name'. Below the field is a reCAPTCHA challenge showing the letters 'P E W F H' in a distorted font. Below the challenge is a button labeled 'Copy the code'. A large green button labeled 'RECOVERY' is centered below the button. Below the button is a link 'BACK'. At the bottom, there is a link 'Alternative login methods'.

Continue

Password reset

3. E-mail which contains the link for password reset is sent and user is redirected back to the login page.
4. After clicking the link in the e-mail, user is redirected to the page for setting new password.
5. Notification about successful password change is displayed.



 **ŠKODA**

NEW PASSWORD SETTING

User
Name Surname

SAVE

NEW PASSWORD SETTING

Your password has been successfully changed, now it is possible to log in.

Certificate installation

Internet Explorer

Mozilla Firefox



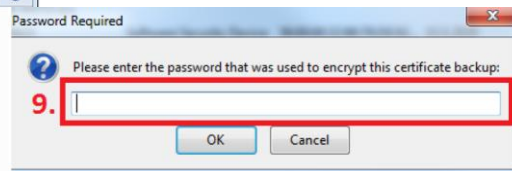
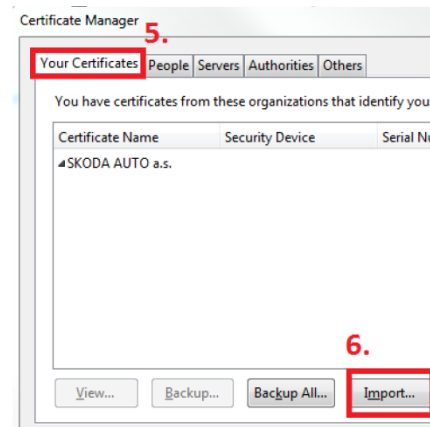
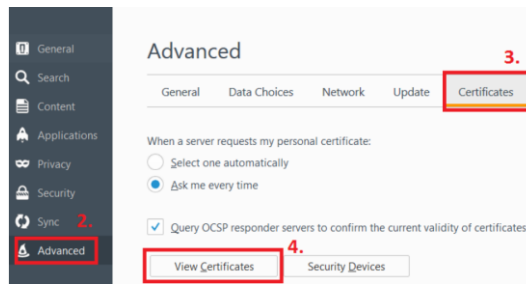
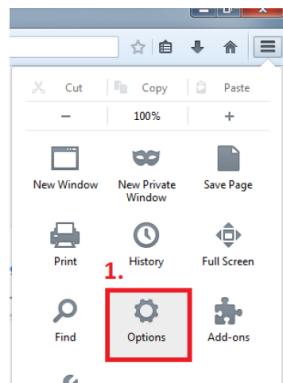
Internet Explorer – certificate installation

The following steps illustrate the process of installing a certificate in Internet Explorer:


- 1) Internet options
- 2) Certificates
- 3) Import
- 4) Next
- 5) Browse
- 6) Choose *.pfx*.p12 and choose your certificate
- 7) Open
- 8) Enter password from PDF file
- 9) Next
- 10) Choose automatically...
- 11) Next on next screen again
- 12) Finish



Mozilla Firefox – certificate installation



- 1) Options
- 2) Extended
- 3) Certificates
- 4) Certificates
- 5) Personal
- 6) Import
- 7) Find your certificate
- 8) Open
- 9) Enter password from PDF file
- 10) OK

 ŠKODA

Request for establishment,
modification or cancellation of
access to B2B

☐ Access establishment ☐ Access modification ☐ Access cancellation


Required access to:

| Information about user | |
|--|-------------|
| Surname: | First name: |
| User ID: | |
| Business number: | |
| Company name: | |
| Address: | |
| Phone: | |
| e-mail: | |
| Reason: | |
| Description of required type of permission (role): | |

| | |
|--|--|
| User | <u><i>Classified information</i></u> yes <input type="checkbox"/> no <input type="checkbox"/> |
| Date | signature |
| Control of user's integrity* | Approved by (superior of user) |
| yes <input type="checkbox"/> no <input type="checkbox"/> | signature, name stamp, stamp |
| <u><i>For employees of external companies</i></u> | |
| User of external company confirmed preservation of confidential information | Head of OU (submitter) |
| | Date: |
| | signature, name stamp, stamp |

| | | | |
|-------------|------|------------|-----------|
| Establisher | name | department | signature |
|-------------|------|------------|-----------|

* => Checks a file in the superior of user, in case of confidential information

** =>  in only in unusual cases

Please send fully filled form via email (B2Bhelp@skoda-auto.cz)
or with internal mail to VMM department

User is obliged to care about safety of data according to regulations "Protection and safety of data" and "Sustaining a confidential information".

In case of any questions or special suggestions, please contact User Help Desk - tel. 19100.

SKODA AUTO s.r.o. 1703

SKODA AUTO s.r.o., Tl. Václava Klementa 868, 283 06 Mladá Boleslav, Czech Republic

ŠKODA

Login

Rules for code from SMS

- Max. number of attempts is 8.
- The interval for checking number of attempts is 1 hour.
- Sending SMS is possible max. 3-times a day
- Password is valid for 15 minutes (if you don't login with this password within 15 minutes of receiving the message, password will expires and you will have to send your SMS with a one-time password again)
- After using this one-time password from SMS, You won't be verified by this password again within one day (24 hours), however you have to be verifying on the same device. For another login you will use only Login + your password to B2B Portal.

Rules for code from Authenticator

- Max. number of attempts is 8.
- The interval for checking number of attempts is 1 hour.
- After using this one-time password from Authenticator, You won't be verified by this password again within one day (24 hours), however you have to be verifying on the same device. For another login you will use only Login + your password to B2B Portal.
- For user verification is necessary to have exact time on mobile device.

Login for 24 hours

- The expiration time for SMS code or Authenticator is 24 hours. Within one day you're no longer asked for two-factor authentication – you're logged in if basic credentials are inserted (Username + password) and SMS or Authenticator method is selected. You can use this feature if you're using the same device (PC, Tablet...).

Continue



ŠKODA

Login

Expiration time for Password recovery link

- The expiration time for password recovery link is 24hours. In case the link is already used / expired appropriate message is displayed and the recovery process must ne repeated.

Fingerprint2

- In case you use Adblock which is set for blocking Fingerprint2 library, the feature of login for 24 hours is lost and you will be asked for SMS or Authenticator code.



Registration

Rules for one-time password

- Sending SMS is possible up to 3 times.
- Password is valid for 15 minutes.

Rules for verification code

- Stays in printer for 24h. After this time it is necessary to send the key again.
- Code is valid for 2 days.
- If you have more devices registered, all keys, that have validity longer than 2 days, will be sent. It is not defined, which key belongs to which device. You can use the key only once and with arbitrary device.

