LOGIN TO MPG-WIDE IT SERVICES VIA MPG-SSO

1. **Enter the URL of the IT service in your browser.**
2. **You will be redirected to the page for selecting the possible authentication methods in the context of the MPG-SSO:**
   - Option 1: Classic login via user name and password ("Classic login with password" section)
   - Option 2: Use of different methods for multi-factor authentication ("Strong authentication" section)

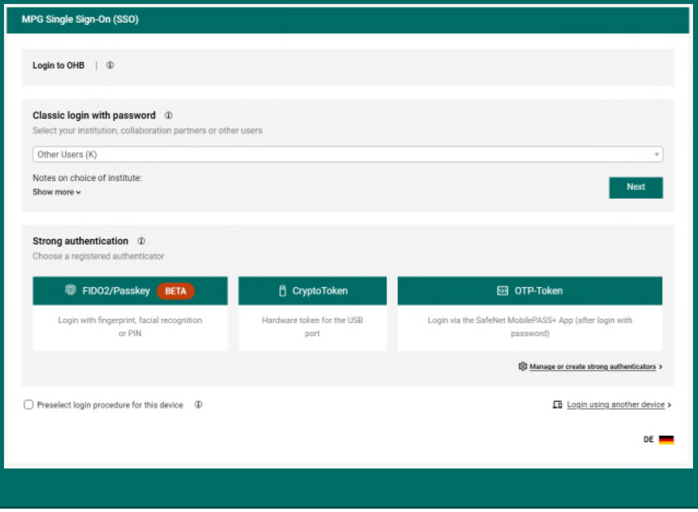
   The following authenticators can be used for multi-factor authentication (MFA):
   - FIDO2/Passkey Token
   - CryptoToken (administrative users only)
   - OTP token via SafeNet MobilePASS+ App

   Note: You must register the above authenticators in the IdPortal (https://idportal.mpg.de) before using them for the first time. The use of other tokens, e.g. such that have been issued by your institute, is not possible!

REGISTRATION TO MAX-PLANCK-WIDE IT-SERVICES

Please use the URL of the desired IT service, e.g:

https://max.mpg.de
https://ohb.mpg.de
https://extranet.mpg.de
https://sbportal.sap.mpg.de
https://bwportal.sap.mpg.de
...



MPG Single Sign-On (SSO)

Login to OHB

Classic login with password

Select your institution, collaboration partners or other users

Other Users (K)

Notes on choice of institute:

Strong authentication

Choose a registered authenticator

FIDO2/Passkey BETA — Login with fingerprint, facial recognition or PIN

CryptoToken — Hardware token for the USB port

OTP-Token — Login via the SafeNet MobilePASS+ App (after login with password)

□ Preselect login procedure for this device

Show more
Next
Manage or create strong authenticators
Login using another device
DE

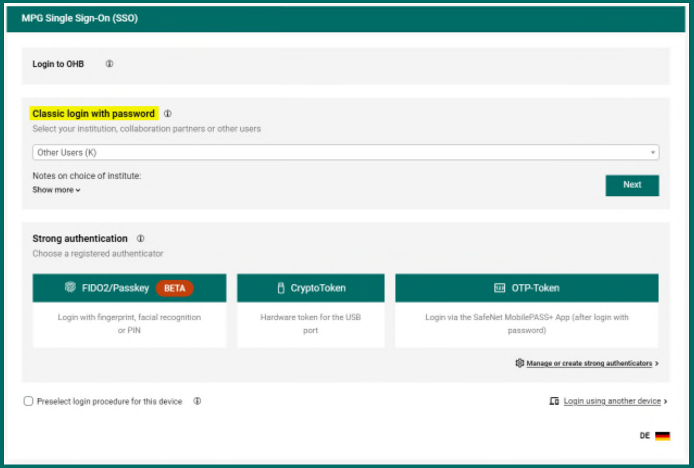
OPTION 1 - CLASSIC LOGIN WITH PASSWORD

CLASSIC LOGIN WITH PASSWORD

1. **To log in with a password without using multi-factor authentication, use the "Classic login with password" section.**
2. **Select your institute from the drop-down list.**
   If you have been invited to a team room as an external user, select "Collaboration partner" from the list.
   If neither of these apply, select "Other users". All persons working for the MPG can authenticate themselves in this way, regardless of their affiliation.
3. **Once you have made your selection, you will be redirected to a login page. Please note the information on the login data to be used there.**

CLASSIC LOGIN WITH PASSWORD

Please use the institute selection in the "Classic login with password" section:



MPG Single Sign-On (SSO)

Login to OHB ⓘ

Classic login with password ⓘ

Select your institution, collaboration partners or other users

Other Users (K)

Notes on choice of institute:

Show more ⌄

Strong authentication ⓘ

Choose a registered authenticator

Login with fingerprint, facial recognition or PIN

Hardware token for the USB port

Login via the SafeNet MobilePASS+ App (after login with password)

Manage or create strong authenticators ›

□ Preselect login procedure for this device ⓘ

Login using another device ›

DE

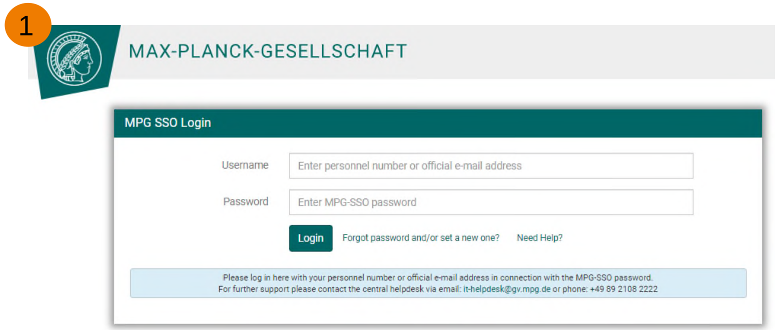
CLASSIC LOGIN WITH PASSWORD

(1) VIA THE CENTRAL LOGIN PAGE

1. **If you have been redirected to the central "green" login page after selecting the list entry, log in here using your personnel number or official e-mail address in conjunction with the MPG-SSO password.**

2. **Change your password if necessary.**

3. **For further assistance, please contact the central helpdesk at e-mail: it-helpdesk@gv.mpg.de or phone: +49 89 2108 2222**



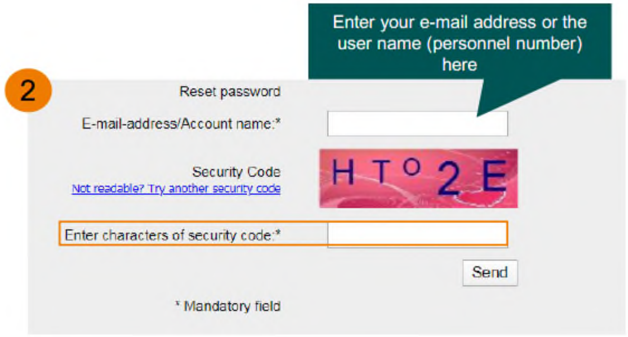
MAX-PLANCK-GESELLSCHAFT

MPG SSO Login

Username: Enter personnel number or official e-mail address

Password: Enter MPG-SSO password

Please log in here with your personnel number or official e-mail address in connection with the MPG-SSO password.
For further support please contact the central helpdesk via email: it-helpdesk@gv.mpg.de or phone: +49 89 2108 2222



Enter your e-mail address or the user name (personnel number) here

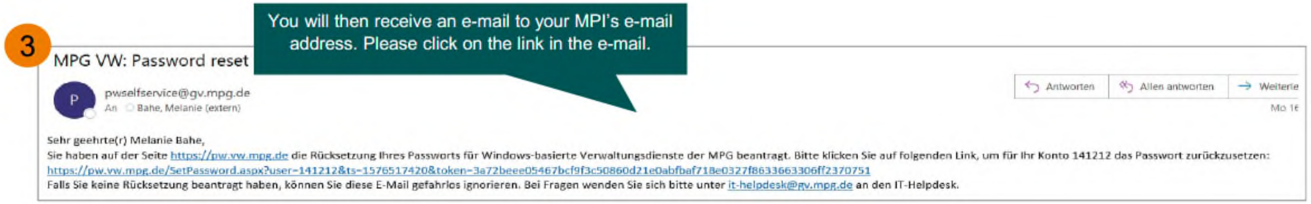
Reset password

E-mail-address/Account name:*

Security Code
Not readable? Try another security code

Enter characters of security code:*

* Mandatory field



You will then receive an e-mail to your MPI's e-mail address. Please click on the link in the e-mail.

MPG VW: Password reset

pwselfservice@gv.mpg.de
An Bahe, Melanie (extern)

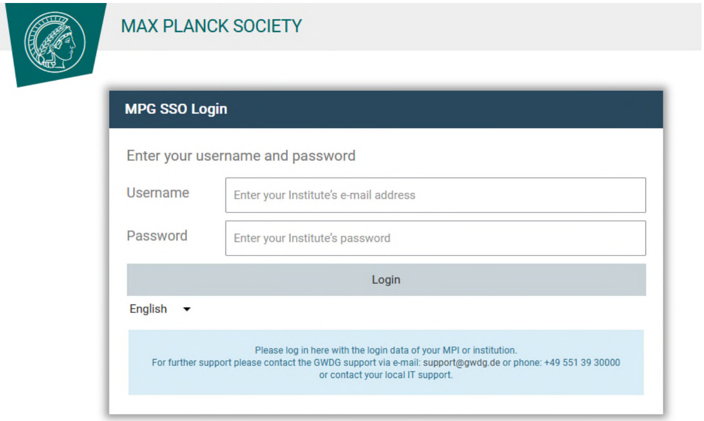
Sehr geehrte(r) Melanie Bahe,
Sie haben auf der Seite https://pw.vw.mpg.de die Rücksetzung Ihres Passworts für Windows-basierte Verwaltungsdienste der MPG beantragt. Bitte klicken Sie auf folgenden Link, um für Ihr Konto 141212 das Passwort zurückzusetzen:
https://pw.vw.mpg.de/SetPassword.aspx?user=141212&ts=1576517420&token=3a72beee05467bcf9f3c50860d21e0abfbaf718e0327f8633663306ff2370751
Falls Sie keine Rücksetzung beantragt haben, können Sie diese E-Mail gefahrlos ignorieren. Bei Fragen wenden Sie sich bitte unter it-helpdesk@gv.mpg.de an den IT-Helpdesk.

CLASSIC LOGIN WITH PASSWORD

(2) VIA THE LOGIN PAGE OF THE GWDG SSO SERVICE

1. If you have been redirected to the "blue" login page of the institute login service of the GWDG after selecting the list entry, log in here with the login data of your MPI or institution (institute login data).

2. For further support, please contact the GWDG support at e-mail: support@gwdg.de or phone: +49 551 39 30000 or ask your local IT support.

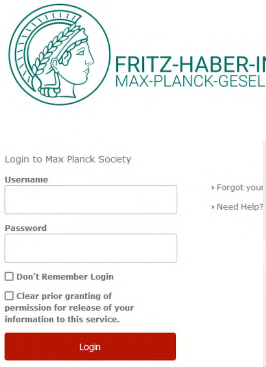

MAX PLANCK SOCIETY
MPG SSO Login
Enter your username and password
Username
Enter your Institute's e-mail address
Password
Enter your Institute's password
Login
English

Please log in here with the login data of your MPI or institution.
For further support please contact the GWDG support via e-mail: support@gwdg.de or phone: +49 551 39 30000
or contact your local IT support.

CLASSIC LOGIN WITH PASSWORD

(3) VIA THE LOGIN PAGE OF YOUR INSTITUTE

1. **If you have been redirected to the login page of your institute after selecting the list entry, log in here with the login data of your MPI (institute login data).**
2. **For further assistance, please contact your local IT support.**



FRITZ-HABER-INSTITUT
MAX-PLANCK-GESELLSCHAFT

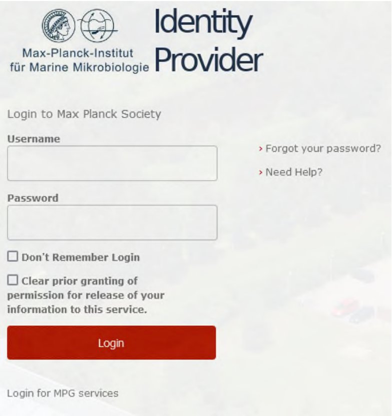
Login to Max Planck Society

Username

Password

□ Don't Remember Login

□ Clear prior granting of permission for release of your information to this service.



Max-Planck-Institut für Marine Mikrobiologie

Identity Provider

Login to Max Planck Society

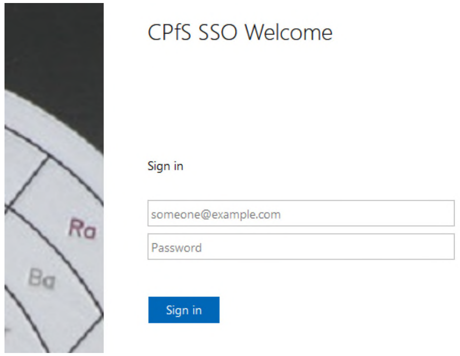
Username

Password

□ Don't Remember Login

□ Clear prior granting of permission for release of your information to this service.

Login for MPG services



CPfS SSO Welcome

Sign in

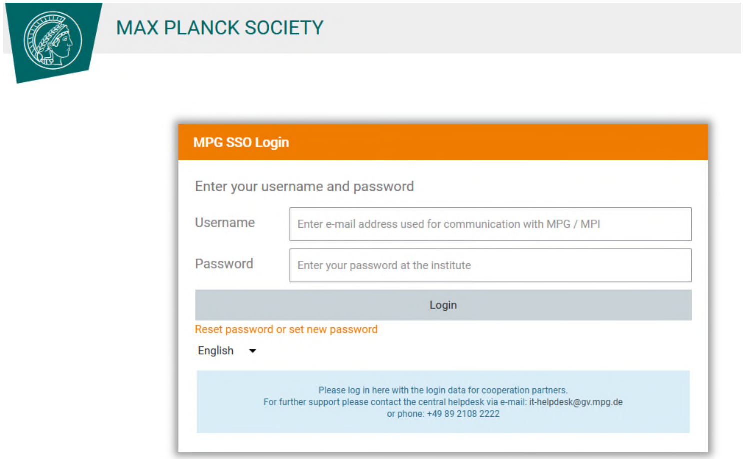
someone@example.com

Password

CLASSIC LOGIN WITH PASSWORD

(4) VIA THE LOGIN PAGE FOR COLLABORATION PARTNERS

1. **If you have been redirected to the "orange" collaboration partner login page after selecting the list entry, log in here using the username from the collaboration partner invitation email in conjunction with the new password you set.**
2. **For further assistance, please contact the central helpdesk by e-mail: it-helpdesk@gv.mpg.de or phone: +49 89 2108 2222**



MAX PLANCK SOCIETY

MPG SSO Login

Enter your username and password

Username: Enter e-mail address used for communication with MPG / MPI

Password: Enter your password at the institute

Please log in here with the login data for cooperation partners.
For further support please contact the central helpdesk via e-mail: it-helpdesk@gv.mpg.de
or phone: +49 89 2108 2222

OPTION 2 - STRONG AUTHENTICATION (MFA)

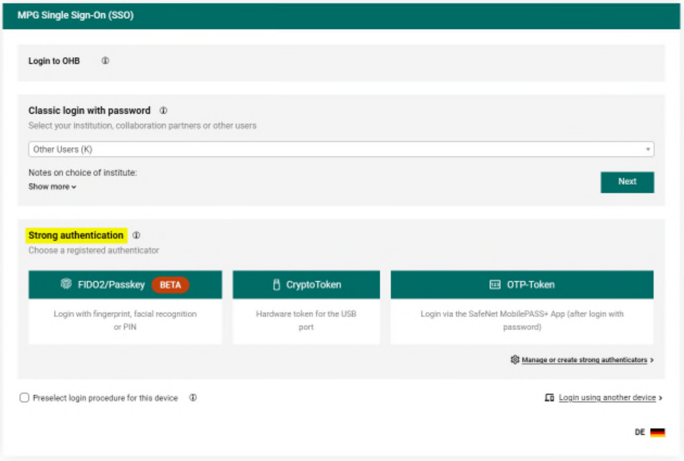
LOGIN VIA STRONG AUTHENTICATION

1. **To log in with multi-factor authentication (MFA), use the "Strong authentication" section.**
2. **Here you can select which of the following three authenticator types you want to use to log in:**
   - FIDO2/Passkey
   - CryptoToken (administrative users only)
   - OTP token via SafeNet Mobile+ App

   Note: You must register authenticators in the IdPortal before using them for the first time. To do this, use the option ⚙ Manage or create strong authenticators › or navigate directly to the URL https://idportal.mpg.de by entering it in your browser
3. **If you have a registered authenticator, select the corresponding authenticator button**

LOGIN VIA STRONG AUTHENTICATION

Please select an authenticator type in the "Strong authentication" section:



MPG Single Sign-On (SSO)

Login to OHB ⓘ

Classic login with password ⓘ

Select your institution, collaboration partners or other users

Other Users (K) ▾

Notes on choice of institute:

Show more ⌄

Next

Strong authentication ⓘ

Choose a registered authenticator

FIDO2/Passkey BETA	CryptoToken	OTP-Token
Login with fingerprint, facial recognition or PIN	Hardware token for the USB port	Login via the SafeNet MobilePASS+ App (after login with password)

⚙ Manage or create strong authenticators ›

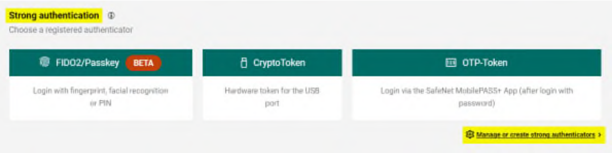
□ Preselect login procedure for this device ⓘ

Login using another device ›

DE

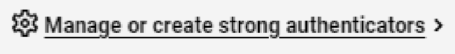
LOGIN VIA STRONG AUTHENTICATION

(PREREQUISITE) MANAGE STRONG AUTHENTICATORS

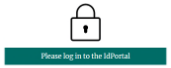


Strong authentication ⓘ
Choose a registered authenticator

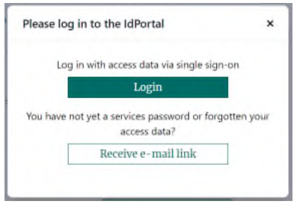
FIDO2/Passkey BETA
Login with fingerprint, facial recognition or PIN
CryptoToken
Hardware token for the USB port
OTP-Token
Login via the SafeNet MobilePASS+ App (after login with password)
Manage or create strong authenticators ›

1. **If you do not yet have an authenticator registered in the IdPortal, click on :** 

   Alternatively, you can navigate directly to the URL https://idportal.mpg.de by entering it in your browser.

2. **On the following page, click on:** 

3. **Log in to the IdPortal via MPG-SSO or email link:**

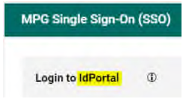
   

   Please log in to the IdPortal ×

   Log in with access data via single sign-on

   You have not yet a services password or forgotten your access data?

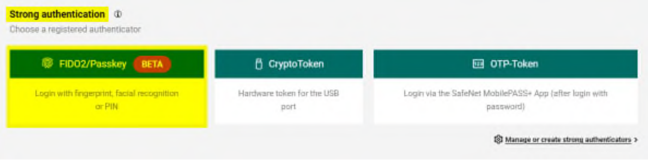
   Note: When logging in via MPG-SSO, the SSO login page will be displayed again, this time for logging in to the IdPortal. Log in here via "classic login with password".

4. **Register the desired authenticator in the IdPortal. Corresponding manuals can be found in the IdPortal or in MAX (https://max.mpg.de/Service/ITServices/Support/Pages/Benutzeranleitungen.aspx) under the topic "IT security" in the sections "FIDO2 token", "CryptoToken" or "OTP token".**

LOGIN VIA STRONG AUTHENTICATION

(1) FIDO2/PASSKEY



Strong authentication

Choose a registered authenticator

Login with fingerprint, facial recognition or PIN

Hardware token for the USB port

Login via the SafeNet MobilePASS+ App (after login with password)

1. **If you want to log in with your FIDO2 token/passkey as strong authentication method, click on "FIDO2/Passkey“.**

A large number of different authenticator variants for FIDO2/Passkey on different technical platforms and devices exists. Here are some examples:

- Windows Hello with biometric authentication or a USB FIDO2 hardware token
- On smart devices, passkeys with biometric login via the screen lock (e.g. FaceID)
- On smart devices with NFC readers wirelessly via a FIDO2 token with NFC support

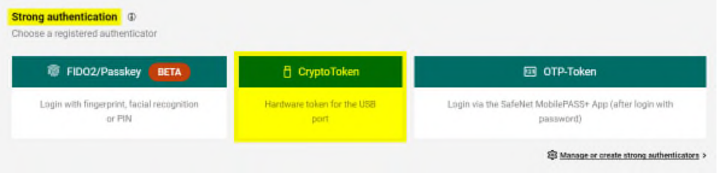
Biometric authentication is usually carried out using facial recognition (assuming a suitable camera) or a fingerprint scanner. The biometric information is usually stored and synchronized on the device. Existing FIDO2 hardware tokens can be used or purchased to meet your own requirements (Yubikey or Gemalto newer model recommended).

Therefore, a detailed description of the individual login methods is not possible. Provided the authenticator has already been successfully registered in the IdPortal, the login process itself is generally not very complex and in most cases almost self-explanatory.

LOGIN VIA STRONG AUTHENTICATION

(2) CRYPTOTOKEN

1. **If you want to log in with your CryptoToken as strong authentication method, click on "CryptoToken".**



Strong authentication

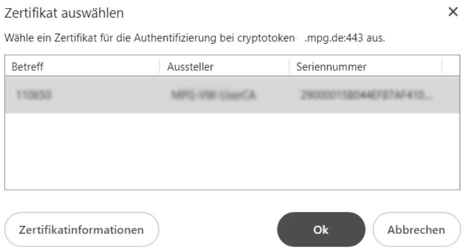
Choose a registered authenticator

Login with fingerprint, facial recognition or PIN

Hardware token for the USB port

Login via the SafeNet MobilePASS+ App (after login with password)

2. **A window will then appear in which you are asked to select the certificate you want to use for login.**
   Click on the certificate and confirm your selection with "Ok".



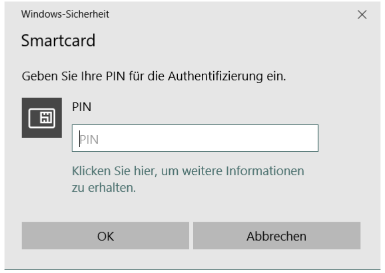
Zertifikat auswählen

Wähle ein Zertifikat für die Authentifizierung bei cryptotoken .mpg.de:443 aus.

Betreff	Aussteller	Seriennummer
[redacted]	[redacted]	[redacted]

3. **A Windows security window pops up, that asks for your certificate PIN. Please enter your certificate PIN here.**

4. **Once you have entered the PIN correctly, you are successfully logged in to the desired service.**



Windows-Sicherheit

Smartcard

Geben Sie Ihre PIN für die Authentifizierung ein.

PIN: PIN

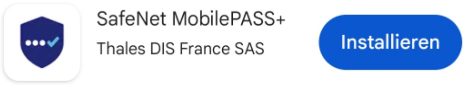
Klicken Sie hier, um weitere Informationen zu erhalten.

Note: CryptoTokens are only issued to administrative personnel!
The login method via CryptoToken can only be used by this user group.

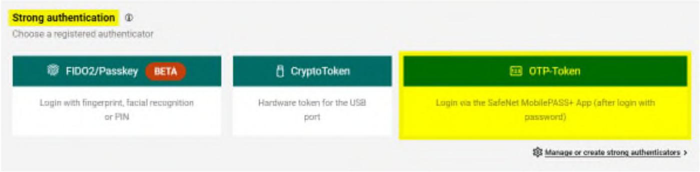
LOGIN VIA STRONG AUTHENTICATION

(3) OTP TOKEN VIA SAFENET MOBILPASS+ APP

Prerequisite: The SafeNet MobilePASS+ app is installed on your smartphone.
You can download the app from your app store.


SafeNet MobilePASS+
Thales DIS France SAS

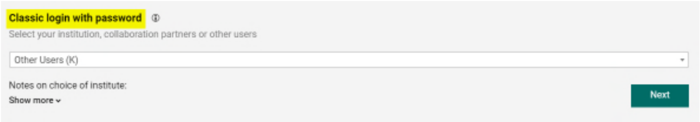
1. **If you want to log in with your OTP token via the SafeNet MobilePASS+ app as strong authentication method, click on "OTP token“.**
2. **In the first step, you must log in with user name and password (see slide 3 ff).**
3. **After having performed the classic login, the authentication request will be sent to the SafeNet MobilePASS+ app and you will be asked to confirm the authentication request in the app.**
4. **As soon as you have confirmed the request via your smartphone, you can access the desired service.**


Strong authentication ⓘ
Choose a registered authenticator

FIDO2/Passkey BETA
Login with fingerprint, facial recognition or PIN

CryptoToken
Hardware token for the USB port

OTP-Token
Login via the SafeNet MobilePASS+ App (after login with password)


Classic login with password ⓘ
Select your institution, collaboration partners or other users

Other Users (K)

Notes on choice of institute:

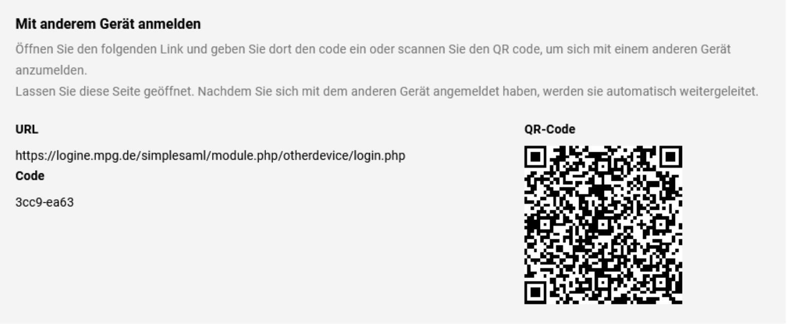
LOGIN VIA OTHER DEVICE

LOGIN VIA OTHER DEVICE

Sometimes it is advantageous to log in to an MPG-wide IT service via the MPG-SSO using a different device, e.g. because a convenient biometric login is possible there or a multi-factor authenticator has not yet been set up on the current device. Even when using a third-party PC, logging in via your own smartphone, for example, is usually easier and more secure.

To do this, you can select the "Log in with another device" option on the page for selecting the available authentication methods. If you have successfully logged in via the other device, you are also logged in on the original device. Proceed as follows:

1. Click on the option Login using another device ›
   You will then see a page with specific information on how to transfer the logon process to the other device.
2. Scan the QR code with a smart phone or enter the URL in combination with the code in the browser of the other device.



Mit anderem Gerät anmelden

Öffnen Sie den folgenden Link und geben Sie dort den code ein oder scannen Sie den QR code, um sich mit einem anderen Gerät anzumelden.
Lassen Sie diese Seite geöffnet. Nachdem Sie sich mit dem anderen Gerät angemeldet haben, werden sie automatisch weitergeleitet.

URL

https://logine.mpg.de/simplesaml/module.php/otherdevice/login.php

Code

3cc9-ea63

QR-Code

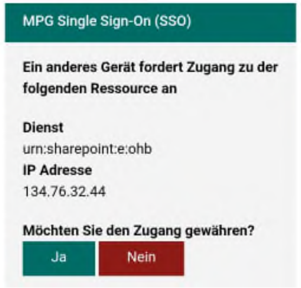
LOGIN VIA OTHER DEVICE

3. On the other device you are asked, whether you want to grant access to the original device or not.
   Click on Yes

4. Then log in via the other device using one of the available login options (classic login / MFA).

5. After successful authentication, you will see a message on the other device, that indicates that the authentication has been completed successfully.

6. In the background, the information about the successful authentication on the other device is forwarded to your original device. On to the original device, you will then be automatically logged in so that you can use the desired MPG-wide IT service there.

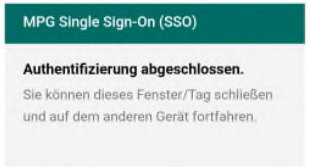


MPG Single Sign-On (SSO)

Ein anderes Gerät fordert Zugang zu der folgenden Ressource an

Dienst
urn:sharepoint:e:ohb
IP Adresse
134.76.32.44

Möchten Sie den Zugang gewähren?



MPG Single Sign-On (SSO)

Authentifizierung abgeschlossen.
Sie können dieses Fenster/Tag schließen und auf dem anderen Gerät fortfahren.

CONFIGURING THE PERSONAL MPG-SSO OPTIONS

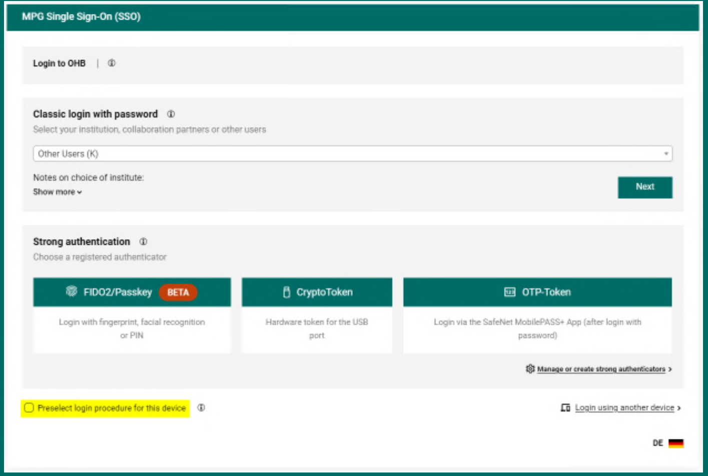
CONFIGURING THE PERSONAL MPG-SSO OPTIONS

1. **The following options are available for managing your personal MPG SSO configuration:**
   - Preselect the login procedure for this device (checkbox beneath the "Strong authentication" section: □ Preselect login procedure for this device)
   - Resetting an authenticator preselection once made (via separate configuration portal)
   - Deactivation of any centrally configured automatic forwarding to an identity provider (authenticating body) based on IP address (via separate configuration portal)

Note:
You can access the configuration portal using the corresponding link on the landing page of the MPG SSO service (https://login.mpg.de). A direct call is possible via the URL https://login.mpg.de/options

CONFIGURATION OF THE MPG-SSO OPTIONS

Please use „Preselect login procedure for this device" option and the configuration portal, accessible via https://login.mpg.de



MPG Single Sign-On (SSO)

Login to OHB | ⓘ

Classic login with password ⓘ

Select your institution, collaboration partners or other users

Other Users (K)

Notes on choice of institute:

Show more ⌄

Next

Strong authentication ⓘ

Choose a registered authenticator

FIDO2/Passkey BETA – Login with fingerprint, facial recognition or PIN

CryptoToken – Hardware token for the USB port

OTP-Token – Login via the SafeNet MobilePASS+ App (after login with password)

Manage or create strong authenticators ›

○ Preselect login procedure for this device ⓘ

Login using another device ›

DE

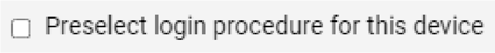
CONFIGURING THE PERSONAL MPG-SSO OPTIONS

(1) SELECT LOGIN PROCEDURE FOR CURRENT DEVICE

Background:

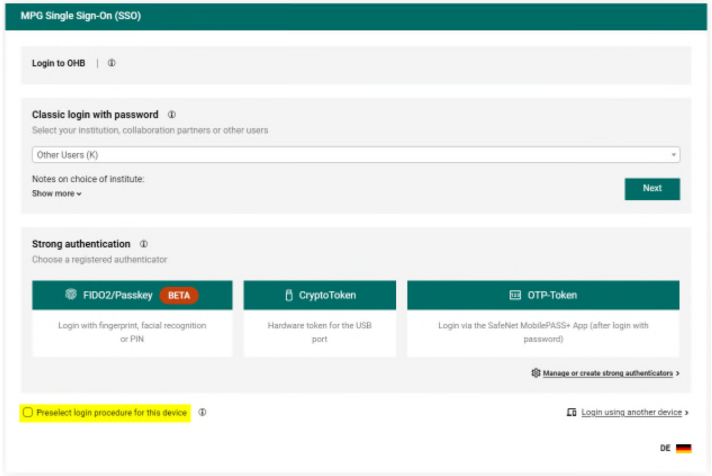
Per device plus browser combination, you can make one of the login procedure (i.e. classic login with password, FIDO2/Passkey, CryptoToken or OTP via SafeNet MobilePASS+ App) your default one. This procedure will then be used automatically for all future logins from the specific browser on the specific device.

1. **Click the check box “Preselect login procedure for this device” directly beneath the “Strong authentication” section:**

   □ Preselect login procedure for this device

2. **Log in using the desired authentication procedure. For all future logins from the specific device and browserbvia which the checkmark was set, the selected login method will be used.**



MPG Single Sign-On (SSO)

Login to OHB | ⓘ

Classic login with password ⓘ

Select your institution, collaboration partners or other users

Other Users (K)

Notes on choice of institute:

Show more ⌄

Next

Strong authentication ⓘ

Choose a registered authenticator

FIDO2/Passkey BETA

Login with fingerprint, facial recognition or PIN

CryptoToken

Hardware token for the USB port

OTP-Token

Login via the SafeNet MobilePASS+ App (after login with password)

Manage or create strong authenticators ›

○ Preselect login procedure for this device ⓘ

Login using another device ›

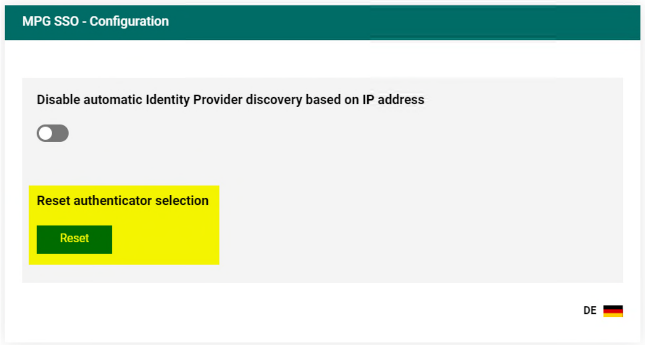
DE

CONFIGURING THE PERSONAL MPG SSO OPTIONS

(2) RESETTING THE PRESELECTED LOGIN PROCEDURE

Background:

If you have configured a standard login procedure for a device (see previous page) and would like to delete this preselection, you can do this via the configuration portal:



MPG SSO - Configuration

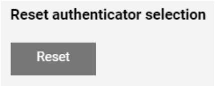
Disable automatic Identity Provider discovery based on IP address

○

Reset authenticator selection

1. **Call the configuration portal via the device you want to delete the preselection for. Use the link on the landing page of the MPG SSO service (https://login.mpg.de) to do so.**
   A direct call is possible via https://login.mpg.de/options

2. **Click on the green "Reset" button. This is then displayed in gray again:**



Reset authenticator selection

The preselection is now deleted. The next time you call a service integrated in MPG-SSO from this device, the page for selecting the possible authentication procedures is displayed again.

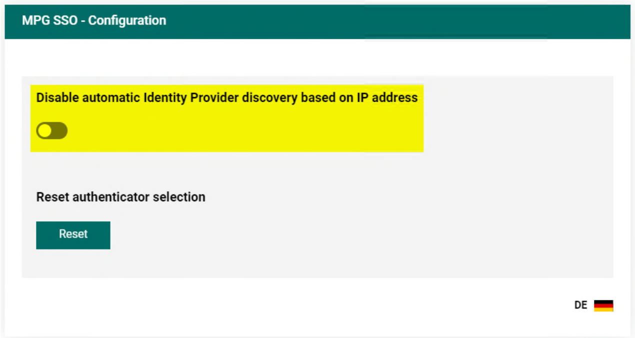
CONFIGURING THE PERSONAL MPG-SSO OPTIONS

(3) DEACTIVATION OF AUTOMATIC FORWARDING

Background:

Depending on the individual situation at the MPI, an IP-based automatic forwarding directly to the SSO login page of your institute may be implemented. In such a configuration, the SSO page with the strong authentication options is never displayed. In order to be able to use multi-factor authentication nevertheless, the automatic forwarding mechanisms have to be deactivated:

1. **To do this, call up the configuration portal via the link on the on the landing page of the MPG-SSO service (https://login.mpg.de). A direct call is possible via https://login.mpg.de/options**
2. **Set the slide button to active, so that the color changes from grey to green:**
3. **The next time you call up a service integrated in MPG-SSO you will be redirected to the page for selecting the possible login procedures again.**



MPG SSO - Configuration

Disable automatic Identity Provider discovery based on IP address

Reset authenticator selection

KNOWN RESTRICTIONS

KNOWN RESTRICTIONS

User groups:

- CryptoTokens are only issued to administrative personnel. They can therefore not be used by institute users.
- For technical reasons, collaboration partners are currently unable to register authenticators in the IdPortal. Therefore, they are generally unable to use strong authentication procedures at present.

Technology:

- To use FIDO2/Passkey on iPhones, keychain synchronization in the iCloud has to be enabled. For this reason, it is not yet possible to use FIDO2/Passkey on GV iPhones, for example.
- Windows Hello has to be enabled under Windows in order to be able to use FIDO2 authenticators. This is not yet the case on the MPG laptops of the GV.
- The use of FIDO2/Passkey is not supported by Samsung Internet Browser.