
CAS user account and password

To ensure that every student and employee of Charles University can use all its online services, they need a **User Account** within the Central Authentication Service (**CAS**).

A CAS account represents your **electronic identity** – it allows you to securely access the services of Charles University using a **single sign-on**. This means you don't need to remember different passwords for the Student Information System (SIS), university email, libraries, or other applications — CAS handles it for you.

What do you need advice on?

CAS User Account

How do I obtain a CAS account?

- Every student and employee automatically receives CAS account when they are admitted to Charles University. Applicants receive one during the admission procedure.
- During your first login to CAS, we recommend that you **set a password** and also configure a **backup recovery method** (telephone number or email), so your account can be easily restored if you forget your password.

What is the CAS account used for?

Your CAS account is your electronic identity and is used to verify your identity when accessing applications or information systems of Charles University (and external systems):

- university applications
- faculty information systems,
- logging in to PCs,
- password management for other systems:
 - for eduroam and dormitory networks
 - domain **JINONICE**
- eduid.cz federation, enabling access to many service providers, especially:
 - issuing personal certificates TCS ,
 - CU electronic resources portal
- medical education portals - MEFANET ,
- e-learning system - Moodle .

What are the advantages of a CAS account?

- One login for multiple university services.
- Higher security – central authentication protected by a password (and optimally two-factor authentication).
- Easier account management – password changes apply automatically across all services.

Why use two-factor authentication and how does it work?

To increase the security of your CAS account, we recommend enabling two-factor authentication .

During login, after entering your password, you must confirm your identity through a second method - usually via CU Key mobile app .

Apart from the CU Key, you can use other methods of two-factor authentication, e.g. hardware key or verification via text message .

The university is currently in the process of implementing mandatory use of two-factor authentication during logging in to university systems.

How do I log in to CAS?

To log in to CAS , use your personal university number (eight-digit number located on your CU card below your photo).

Enter your password — either your current one or the initial password issued by the CU card issuing center .

How do I find my username?

Your CAS username is your eight-digit personal university number, found:

- on your CU card below your photo,
- in the email you received when you first set your CAS password.

I can't log into CAS — what should I do?

I forgot my password or it's not working

There may be several reasons for why you cannot log into CAS — forgotten password, expired password, or a compromised account.

Recommended steps:

Try resetting your password online

- The fastest way is to visit [password recovery portal](#) .
- After verifying your identity (email, SMS, NIA), you can set a new password.

Visit a service office — if online recovery is not possible

- If online password recovery fails, visit [CU card issuing center](#) or an [authorized faculty office](#) .
- You will receive an **initial password**, which must be changed within 5 days.

Suspicion of account compromise

- If you suspect misuse (unusual activity, unknown logins), immediately contact the [CU CSIRT team](#) .

Important: *Even after changing your password, your data may remain accessible on devices where you were previously logged in, so **always report suspected incidents** .*

I can't log in even though my credentials are correct

Try closing old browser sessions, clearing cache/cookies, or using another browser.

Where can I get help?

Use the [Login issues](#) form in ServiceDesk.

CAS Password – setup, change, recovery

Setting and changing your password

What is the initial password and where do I get it?

The **first initial password** to the Central Authentication Service (CAS) was assigned to you and issued when you issued your [CU card](#) or at your request (e.g. when losing your password or when replacing an unverified password), either by the [CU card issuing centre](#) or by [authorized faculty office](#) .

The initial password is used **ONLY to set the password** (so-called verified) to [CAS](#) . It cannot be used for logging into other CU information systems.

It is valid for 5 calendar days only. After the expiry of this period, it becomes null and void and cannot be extended or reused in any way.

How do I change my initial password and set my own?

- It is not necessary to visit the CU Card issuing centre to set a new password. You can change your password yourself after logging in.
 - Firstly, you must log in to [CAS](#) .
 - Use the university personal number (eight digits) under your photo on the [CU card](#) as your login name.
 - In the "**Password**" box, enter your **initial password** assigned by the CU Card issuing centre or by the authorised faculty office.
 - After logging in, go to the menu item on the left "Password for CAS" and select "[Change the initial password](#) " .
 - Set your **NEW - verified password** here. The rules that a new password must comply with are always clearly listed here.
- **If you do not know** or have forgotten your password, follow the chapter "**I forgot my password or it doesn't work**"

What password to choose?

The rules for creating a suitable password are directly defined after logging in to your CAS account (in the [New Password setting](#) step).

How often to change your password?

- Although the password is well thought out and strong, the longer it is used, the more likely it is to be broken through, which can lead to misuse of your account. It is therefore recommended to [change your password regularly](#) .
- Within the CAS access rules, this is once a year. You will be informed by email about the need to change your password in time (one month in advance). The email will also indicate the exact expiry date of your old password.

How do I extend the validity of my password?

You can [extend the validity](#) of your password by **changing your password**. If your faculty policy allows it, you can reuse your original password as well.

How to handle the password?

- Be careful when entering your password and pay attention to your surroundings.
- Never share your password with others.
- Always log out when logging in on a public internet network.
- Remember your password, if you need to write it down, use applications designed for password management, e.g. [Keepass](#) etc.

How do I change my current password?

- **If you know your current password**, it is not necessary to visit the CU Card Issuing Centre to change/get a new password. You can change your password yourself after logging in.
 - First, you must log in to your [CAS account](#) .
 - Use the university personal number (eight digits) under your photo on the [CU card](#) as your login name.

- In the "**Password**" box, enter your current password, or the initial password assigned by the CU Card issuing centre or by the authorised faculty office.
 - After logging in, go to the menu item on the left "**Password for CAS**" and select "[Change password for CAS](#)".
 - Here you set your **NEW (verified) password**. The rules that the new password must comply with are always clearly listed here.
 - **If you don't know the password** or have forgotten it, follow the section "**Forgot my password or it doesn't work**"
- The CAS password has expired - how should I proceed?
- The password expiry date information was sent to your email address a month in advance. After this period, the password will no longer work for logging in to applications, but it can still be changed on the CAS user portal for 6 months.
 - If your password expired less than six months ago (and you still remember it), you can use this password to log in to the CAS portal and [reset your password](#).
 - Otherwise follow the same procedure as if you forgot your password according to the chapter "**Forgotten Password - Password Recovery**"

Forgotten Password - Password Recovery

If you have forgotten your password, you can set a new one through the [Password recovery portal](#).

To verify your identity, use one of the available methods:

Email password recovery

If you have an email address set up in your CAS account, you can [reset your password](#).

SMS password recovery

- If you do not know the valid password, but you have a phone number set for your account, we will verify your identity by sending a check SMS message and you can set a [new password](#).
- If you don't know the password and you don't have a set phone number, you must follow the same procedure as if you don't have a password at all - visit [CU Card issuing centre](#) or [authorized faculty office](#).

Password recovery using NIA

You can also reset your CAS password using the Public Administration tool - [NIA](#).

Password recovery using SvipelD

You can also reset your CAS password using the [SvipelD](#) tool.

Personal visit

If you have forgotten your password, follow the same procedure as if you don't have a password - visit [CU Card issuing centre](#) or [authorized faculty office](#).

Verified and unverified password - what is the difference between them?

You can find information about what type of password you currently have set by logging into [CAS](#) in the **Account Information/Password Type** tab.

What is a verified password and how do I get it?

The **verified password** is the standard and recommended type of password for the CAS account. You get it after verifying your identity.

You can verify your identity in two ways:

- **personal** visit [CU Card issuing centre](#) or [authorized faculty office](#) and presenting a photo CU card,
- **online** through the [portal for remote identity verification](#) and using the [NIA](#), or [SvipelD](#).

A verified password allows you to use **all university systems and services** without restrictions.

What is an unverified password and how do I get it?

An **unverified password** is a password with a lower level of trust. It **only serves as a temporary and emergency solution** if, for some reason, your identity cannot be verified in the standard way.

It can be obtained without a personal visit to the card issuing centre or authorized faculty office. You can set an unverified password online in two ways:

- in the [CAS account](#) via the password reset form, by sending an SMS and e-mail invitation to the contact details registered in CAS,
- in emergency cases using special methods available in the [portal for remote identity verification](#) (only if more trustworthy authentication methods fail).

When setting an unverified password, you are always reminded of this fact.

Important notice: An **unverified password** may restrict you from using certain university services. For example:

- login to all systems may not work,
- cannot set access to the **eduroam** network,
- it may not be possible to apply for a **personal certificate**,
- some faculties only require a verified password.

Therefore, use an unverified password **only temporarily** and set a verified password as soon as possible.

Services requiring verified passwords

- [eduroam network](#),
- domain JINONICE,
- LF computer network in Pilsen (STUDENTS domain),
- [personal certificates TCS](#).

Frequently Asked Questions (FAQ)

I log in to CAS but not to SIS, what should I do?

- You may have been denied access by the app because you lack permission to work with it. You must be a student or a CU employee to join SIS. Especially for candidates after enrolment, it is possible that your study department has not yet modified your relationship in the SIS database and therefore SIS will not allow you to log in, in this case contact the [Faculty Administrator of IS Studium](#) .

I have a problem with multifactor (MFA) authentication.

- In the first step, log into your CAS account and check your Multifactor Authentication settings. If necessary, make a [new setting](#) . Choose from the available methods, we recommend CU Key mobile app and Text message code. Follow the two-factor authentication process.

CAS password cannot be changed - weak password

- The rules for creating a suitable password are directly defined after logging into your CAS account (in the [New Password setting](#) step).

How do I change my contact details?

- You can change your contact details after logging into your [CAS account](#) in the "**Change Contact Information**" section.

Where can I get a verified password?

- The verified password is issued by [CU Card issuing centre](#) or [authorized faculty office](#)

Services requiring verified passwords:

- [Eduroam network](#) ,
- domain JINONICE,
- LF computer network in Pilsen (STUDENTS domain),
- [personal certificates TCS](#) .

Support, Helpdesk

If you have not found an answer to your question on this page, please contact Servicedesk via the [Login issue](#) form.

Important Links

- [Recovering your CAS password via identity verification - NIA](#)
- [Recovering your CAS password via identity verification - SvipeID](#)
- [How to set up a two-factor authentication](#)