

Glossary and explanations regarding the user and group applications at WWU

General information:

- The forms N (Use of computers and IT services at the university), and G (User groups at the university) can be filled out in PDF format on your computer and be printed out in order to be signed. We recommend this procedure as it facilitates the processing.
- By now, most of the members of Westfälische Wilhelms-Universität (WWU) gain **access** to the IT system (including e-mail and Internet) **automatically** via the identity management system. In these cases, a separate application in writing is not necessary and should be **avoided** as it may cause inconsistencies. This holds for:
 - **Students** of the WWU receive fully-fledged access to the ZIV's systems and, if necessary, to certain departmental computer systems on enrolment day. Therefore, activation is not necessary anymore.
 - **Members of staff** being administered by the personnel department of the WWU have a userID which is kept at the personnel department and, if necessary, activated in the hiring process. It is valid until the end of employment.

In these cases, form N is only required for user right extension. The present userID then has to be named.

1. Authorised persons for application

According to the terms of use, the following persons are authorised to apply for the ZIV and the IT support units (IVV).

- Professors, members of staff and students of the WWU and the University Hospital as well as other universities in Münster that do not own IT facilities and are due to special agreements allowed to use the IT services of the WWU,
- staff members of student services,
- staff members of institutions collaborating with the WWU in research matters,
- persons who have a special permission from the head of the ZIV.

Usually, the applications need to be countersigned by a professor, or a head of one of the university's institutions, or their authorised representative (from now on referred to as head of user group).

The applicant is **obliged** to use the IT resources of WWU exclusively for the purposes listed in the [terms of use](#).

2. UserID, log-in name etc.

2.1. Purpose

Those who want to access/use a computer or IT service within the network of the WWU need to have a user permission for the particular computer system. These permissions are granted through the registration of the userID and its attribution to one or more user groups. **The user must log-in into the system with his/her userID.** The identity is confirmed by entering an encrypted **password** being saved in the system (see 3.). As the userID is also used for log-in, it is also called **log-in name**, Windows systems use the term "**Benutzername**", in English-speaking contexts the term "**UserID**" is common. The userID is also part of the **e-mail address** (For alternatives see 4.)

2.2 Scope of application

The ZIV of the WWU creates userIDs and saves them in a central user data base. On enrolment day, students receive a userID from the student office. Members of staff at the WWU receive a userID from the personnel department being valid until the end of employment. Such a userID is registered in the central server systems of the ZIV (Unix-systems, Windows systems (Domain: uni-muenster.de), e-mail, internet access). When associated with certain user groups, the registration can also be done in the departments of psychology, sports, mathematics, information technology and the IT support unit (IVV) for sciences (Physics, chemistry, pharmacy and biology).

Those departments not mentioned here have their own computer systems. Here it should be possible to use the same userID.

2.3 Granting of access

Usually, everyone can only have one userID, but exceptions are possible (see 2.6). It will be given out by the student office, the personnel department or by the ZIV when the first application has been processed – the userID is then saved in the user data base. Belated changes imply great effort and will therefore only be undertaken due to compelling reasons.

One person can apply for an additional userID if this is, for example, necessary for administrative purposes. The identity management system retains the userIDs one person has got.

Normally, the userID given out by the ZIV consists of the surname (in case of compound names only the last part) and parts of the first name, under consideration of the rules stated in 2.4. Suggestions for different userIDs can be made as long as the following rules apply. As about 150.000 userIDs have already been given out, more than one suggestion should be made. In case the first suggestion is already in use, the other suggestions will be needed.

2.4 Rules for the form of the userID

Due to technical and organisational reasons, a userID consists of 2 to 8 standard letters (only lower case letters, except for ä, ö, ü, und ß) and numbers; the first, second and last character can only be letters.

2.5 Access authorisation, validity

Every userID is associated with a least one **user group** of the ZIV according to the application (see 5.). It is possible to extend or change the associated user groups at a later time.

The association with the standard user group for students (u0dawin) and those groups for the use of department computers is valid until exmatriculation. For members of staff at the WWU, being administered by the personnel department, the association with the

- standard user group (u0mitarb),
- as well as further user groups of the institute (department), resulting automatically from the employment,
- as well as further user groups if requested,

are valid until the end of employment.

Usually, the association with a user group expires after 2 years. It can be extended at a request in writing.

The userID and its related personal data will be saved in the database as long as archived files of the user exist – even when the userID has expired; therefore, the userID can be reactivated when registering again.

2.6 Impersonal userIDs

Institutions of the WWU, workgroups, and recognized student groups can apply for impersonal userIDs. In these cases, please fill your desired userID in the appropriate field.

3. Password

3.1 Due diligence

As the user can identify him-/herself by the password, it should be chosen carefully and changed frequently (cp. 3.3); it must not be made accessible to unauthorised persons. The user is fully responsible for any misuse of his userID.

3.2 Setting the initial password

When first registering the userID in the systems mentioned in 2.2, the ZIV or the student office set a initial password. The applicant receives the password in writing, i.e. by the head of the user group or, if no signature of the head of the user group is required, at the ZIV help desk upon presentation of any ID. Due to security reasons, the initial password should be changed immediately after the notification has been received (cp. 3.3).

3.3 Changes

Although the disposal of the userID and changes in data as well as the association with user groups takes place in the ZIV, the computer systems being involved have independent systems for access control. Even if the passwords are therefore stored separately, most of them can be changed synchronically via the user portal [Mein ZIV](#). For the remaining systems, different methods have to be applied – the responsible system administrator will provide you with the required information.

4. E-mail addresses

If the userID includes setting up a mailbox and an e-mail address, the elementary form is userID@uni-muenster.de.

The central mail server of the ZIV can be notified of a further name, i.e. an e-mail alias, via the user portal [MeinZIV](#). This e-mail address can then be used instead of the userID.

5. User groups

The ZIV creates user groups in order to define collective requirements for IT resources, i.e. access to certain computer systems as well as the use of printers and plotters. Within a computer system, the members of a user group form a group in the sense of the particular operating system, i.e. they are having the same access authorisations for certain resources.

User accounts being associated with several user groups have the rights from **all** of these groups. The user authorisation for one computer system expires, when the association of the userID with **all** user groups whose rights include the use of the system has expired.

The ZIV creates user groups for the general tasks in the institutions of the WWU and the student councils as well as the students – these groups are created automatically or if required and have access to the standard resources. For workgroups in departments, user groups with requirements going beyond the standard (e.g. homepage administration), projects predominantly third-party funded etc. user groups can be applied for by a professor of the WWU or a person being in charge of the funding via a special form, namely form G. Applications of users for the association with such a user group can be handed in along with form G.

Also, form G can be used to authorise a further person as head of the user group.

If you have any questions related with the userID and the creation of user groups, please contact admuser@uni-muenster.de [Reinhard Mersch](#)