

SWITCH edu-ID Achievements of the Past Year

SWITCH

Rolf Brugger / Lukas Hämmerle
eduid@switch.ch

Tr&Id WG Meeting, Berne, 15 May 2019

Topics Covered

Many achievements in last year but this presentation focuses on:

- 1. Organisation Administration Interface / Technical Accounts**
- 2. Duplicate Handling**
- 3. Multi-factor Authentication / Two-Step Login**

1. Organisation Administration Interface/Technical Accounts

Organisation Administration Interface

- **Where is it?**

<https://eduid.ch/web/organisation-administrator/>

- **Who is it for?**

- Migrated and non-migrated organisations

- **Who can access it?**

- All Resource Registry Home Organisation/Attribute Release Policy administrators
- Other users can be specifically granted access on request

What functions does it provide?

- Review the most important statistics, status information about organisation in the context of edu-ID
- Inspect, temporarily disable or terminate organisation affiliations of edu-ID users
- Review changes performed by fellow administrators
- Review and manage security, emergency and generic edu-ID service contacts for own organization
- Create and manage technical edu-ID accounts

Technical Accounts

- Special edu-ID accounts for:
 - Testing purposes
 - Monitoring
 - Service accounts
- Can be created via the organization administration interface
- Once created, usable like a regular edu-ID account

Characteristics of Technical Account

Differences to regular accounts

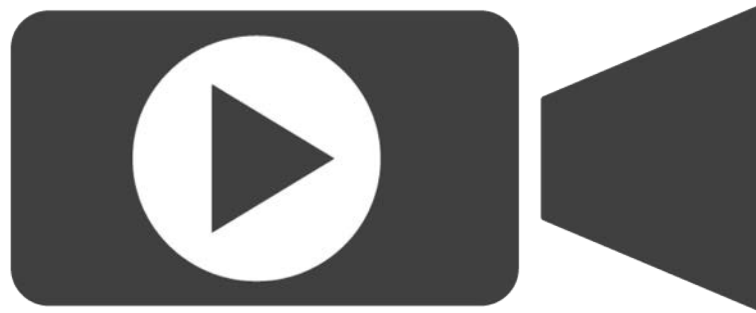
- UniqueID/edu-ID identifier values start with '0000'
- eduPersonEntitlement value always released to service
 - Even if service does not request it
- Entitlement value of the form:
 - <https://eduid.ch/spec/technical-account/#homeOrgName>
 - homeOrgName=ethz.ch, unige.ch, hes-so.ch,
- Account should not represent real person

Management of Technical Accounts

- Owned and managed by organization it was created for
- Admins are reminded twice a year about technical accounts

More information: <https://www.switch.ch/edu-id/organisations/idm/org-admin/>

Demo Organisation Admin/Technical Accounts



2. Duplicate Handling

Some Name Statistics

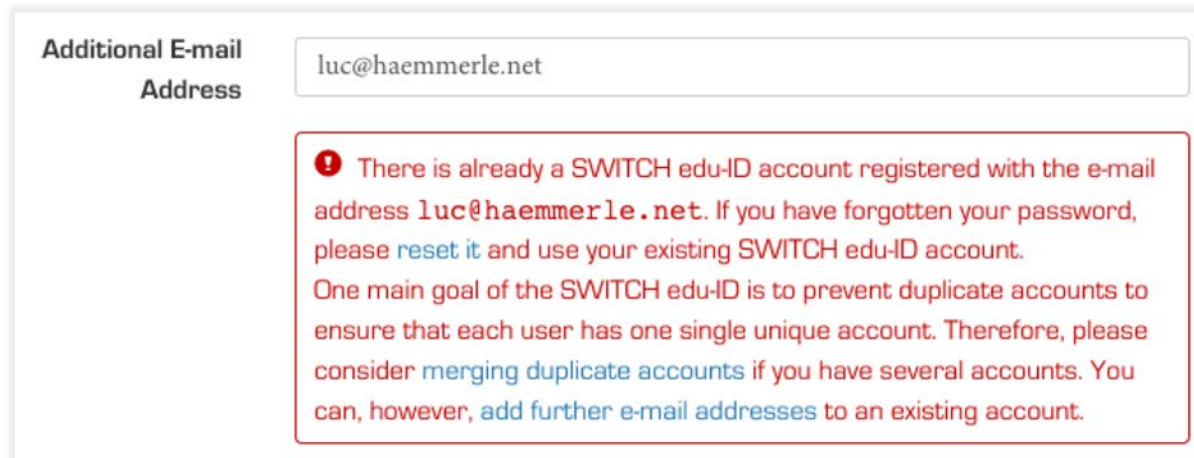
- Currently > 112'910 edu-ID accounts (May 2nd 2019)
- 10'912 names (9.7%) users have non-unique name
 - Ignoring umlaut substitution: Müller != Mueller
 - Ignoring middle names: Samuel Burri != Samuel Luca Burri
- **Most used names:**
 - 11 Thomas Müller, Christoph Müller
 - 10 Matthias Müller, Andreas Meier
 - 9 Lukas Schmid
 - 8 David Schmid, Sarah Baumann
 - 7 Nicole Meier, Lukas Müller, Martin Keller + 9 other names
 - 6 Benjamin Müller, Pascal Schmid, Laura Keller + 21 other names
 - 5 Tobias Huber, Peter Meier, Susanne Schmid + 45 other names
 - 114 Manuel Schmid, Michael Koller, Jürg Roth + 113 other names
 - 485 duplicate users with 3 names
 - 4'208 duplicate users with 2 names

Preventing Duplicates

- It's **impossible** to prevent all duplicates without relying on unique identifier (e.g. social security number)
- **Names cannot be used** reliably and in a data privacy-respecting way
- **Strategy:**
 - Prevent as many duplicates as possible
 - Provide merge process (for admins and users)

Identifying Duplicates

- Adding/linking already associated unique values (mail, mobile number, AAI identifiers, ORCID ID) triggers warning and sometimes email to user if duplicates exist already

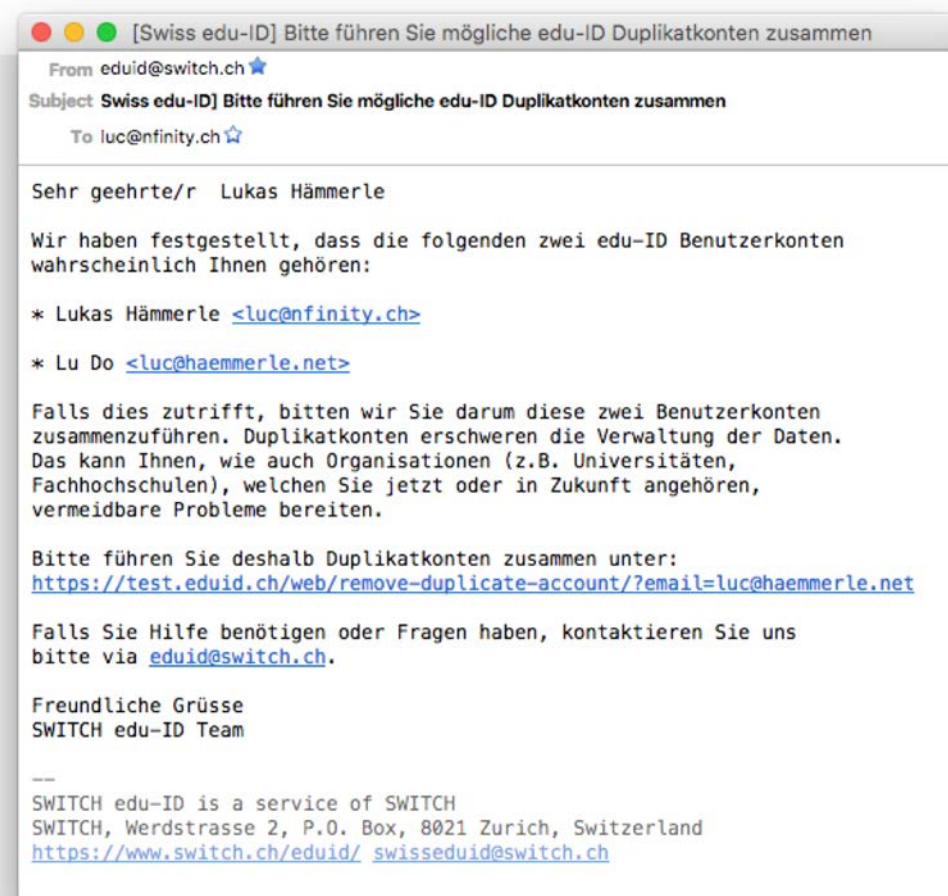


The screenshot shows a form with the label "Additional E-mail Address" and a text input field containing "luc@haemmerle.net". Below the input field is a red-bordered warning box with a red exclamation mark icon. The warning text reads: "There is already a SWITCH edu-ID account registered with the e-mail address luc@haemmerle.net. If you have forgotten your password, please [reset it](#) and use your existing SWITCH edu-ID account. One main goal of the SWITCH edu-ID is to prevent duplicate accounts to ensure that each user has one single unique account. Therefore, please consider [merging duplicate accounts](#) if you have several accounts. You can, however, [add further e-mail addresses](#) to an existing account."

- Sometimes too late to prevent duplicate at this point
 - But user is informed about duplicate merge

Reminder to Deduplicate Accounts

- Sent immediately when duplicate is detected
- Reminder sent 2 weeks later if accounts were not merged



Account Deduplication Goals

- Simple Process
- Secure and Safe without misuse potential
- Accountability
- Automatic SP Admin notification
- Voluntary

Deduplication = Account Merge

1. Accounts merged **by administrator**

- SWITCH could also proactively merge accounts according to Terms of Use (Article 7.e): *“SWITCH reserves the right to merge and/or delete any accounts identified as duplicates, which may lead to loss of data or restricted access to services.”*
- So far a few dozens obvious duplicates were merged

2. Accounts merged **by users themselves** (since May 2018)

- Users are shown link to account merge page or they are reminded via email (previous slide)
- User then can merge accounts on his own as shown on following slides

Account Merge by User: Step 1



You can merge multiple duplicate SWITCH edu-ID accounts on the following pages. When merging two accounts, information from the duplicate account to be removed will be added to the remaining account where this is possible and reasonable. The duplicate account will then be removed.

To start the process, please first provide e-mail address and password of your other account.

This account

E-mail Address

elisabeth.muster@hepl.ch

Other account

E-mail Address

elisabeth.muster@unige.ch

Password

.....



[Forgot password?](#)

How much is:

~~15 + 16 + 5 =~~

36



Cancel

Reset

Proceed

Account Merge by User: Step 2

Authenticate with both accounts 1 Choose account to keep 2 Merge accounts 3

Please select which account you would like to keep. Identity data from the other account will then be merged into the remaining account where possible.

<p>First Name Elisabeth</p> <p>Last Name Muster</p> <p>E-mail Address elisabeth.muster@hepl.ch</p> <p>Account creation date 3. 5. 2017 15:58:19</p> <p>Last login date 5. 6. 2018 08:59:37</p> <p>Accessed services 10</p> <p>Linked active identities 2</p> <hr/> <p><input checked="" type="radio"/> Keep this account</p> <p>(This is the recommended choice)</p>	<p>First Name Elisabeth</p> <p>Last Name Muster</p> <p>E-mail Address Elisabeth.Muster@unil.ch</p> <p>Account creation date 19. 11. 2014 11:48:31</p> <p>Last login date 26. 3. 2018 15:11:25</p> <p>Accessed services 0</p> <p>Linked active identities 1</p> <hr/> <p><input type="radio"/> Keep this account</p>
---	--

Cancel Proceed

Account Merge by User: Step 2.5



Please select which account you would like to keep. Identity data from the other account will then be merged into the remaining account where possible.

<p>First Name Elisabeth</p> <p>Last Name Muster</p> <p>E-mail Address elisabeth.muster@hepl.ch</p> <p>Account creation date 3. 5. 2017 15:58:19</p> <p>Last login date 5. 6. 2018 08:59:37</p> <p>Accessed services 10</p> <p>Linked active identities 2</p> <p>This account will remain</p>	<p>First Name Elisabeth</p> <p>Last Name Muster</p> <p>E-mail Address Elisabeth.Muster@unil.ch</p> <p>Account creation date 19. 11. 2014 11:48:31</p> <p>Last login date 26. 3. 2018 15:11:25</p> <p>Accessed services 0</p> <p>Linked active identities 1</p> <p>This account will be removed.</p>
---	--

Please read before you continue

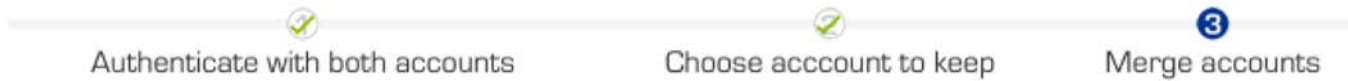
Merging duplicate accounts is generally recommended to avoid access problems in the future. Merging accounts has the following consequences that you should be aware of before continuing:

- The password of the account to be removed will not be transferred to the remaining account. The password for the remaining account that stays the same.
- User settings and content of some services (e.g. SWITCHdrive) that were accessed with the account to be removed might not be available for some time directly after the account is merged. This is because the operators of the respective services might first need to transfer user settings and content to the account that remains. When the account is merged, SWITCH will inform the operators of the affected services and ask them to apply the necessary changes in a timely manner.

Cancel

Merge accounts

Account Merge by User: Step 3



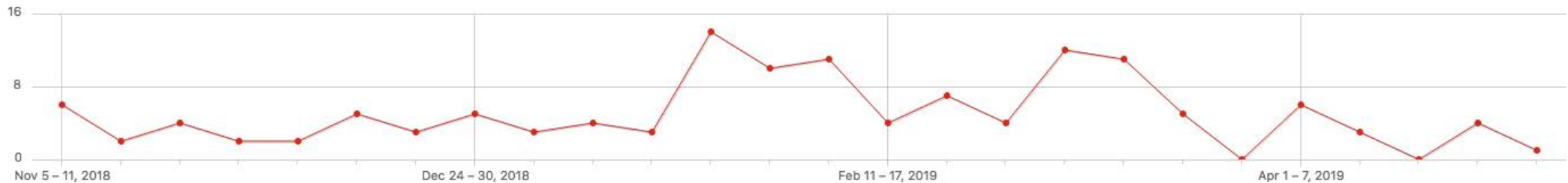
Successful Account Merge

The account merging operation was successful. The details were also sent to your primary e-Mail address `elisabeth.muster@hepl.ch`. Please review your account data to see if your identity data still is correct and up-to-date after the account merging.

[View Account Details](#)

Duplicate Handling Summary

- We try our best to prevent duplicates
 - But not all duplicates can be prevented...



- Merge process to ensure that number of duplicates is low
 - User can merge accounts and is encouraged to do so
 - On average 20 account merges per month initiated by user
 - Side effects of merge have been very low so far

More information: <https://www.switch.ch/edu-id/organisations/idm/duplicates/>

3. Multi-factor Authentication Two-Step Login

Purpose of two-step login

- edu-ID enforces modern password policy
 - NIST 800-63B recommendations
- Additional protection for identity theft (phishing)

SWITCH edu-ID supports

1. Factor - knowledge: password
2. Factor - possession:
 - Mobile phone with **SMS** or **TOTP** app (“Google authenticator”)
 - **backup codes**

When is two-step login required?

If required by service



also for selected user groups

If required by user



may remember 2FA session for one week

If required by organization
(to be developed)



More information: <https://www.switch.ch/edu-id/services/two-step-login/>

Demo MFA/Two-Step Login

