How to change your CERGE-EI accounts passwords

Because of security measure, CERGE-EI distinguishes between network (domain) passwords and mailserver passwords.

As a result, there are different passwords for:

- your **domain account *ad.cerge-ei.cz*** (Active Directory) used for network logon, VPN, web, TAS etc. [D]
- your **Zimbra mail exchange** server account [X]
- your **Zimbra archive mail** server account (if available) [A]

Guidelines

for Domain account [D]

*Username is usualy in the format **nsurname** (first letter of name + surname, max. 8 characters. e.g. jdoe, bsprings, ...). **

There are two basic ways how you can change your domain account:

- **the first way: Windows login page**

Press Ctrl+Alt+Delete → click “Change a password...” , type your old password followed by a new password as indicated, and then type the new password again to confirm it.

- **the second way: Password Self-Service Portal** (experimental)

Go to the address https://portal.cerge-ei.cz/pwm and log with your domain account. You can also **reset forgotten password** if necessary (you have to have your mobile phone registered at the portal in advance to be able reset password via SMS).

* You can find out your username at the self-service portal → click *[Forgotten User Name]* button at the Password Self-Service Portal

(Please note, that there is a transition process of gradual enabling of 'older' user accounts to use this Self-Service Portal. If you wish to use this feature, send your inquiry to HELPDESK and we enable your account for this Self-service portal)

See User Accounts page for more details...

Email Accounts Passwords

for Zimbra email Exchange [X]

Server: https://mail.cerge-ei.cz

Use webmail for Zimbra Password change

for Zimbra Archive [A]

Server: https://mailarch.cerge-ei.cz(experimental/pilot phase)

PWMA - Self-service Portal Go to the address https://portal.cerge-ei.cz/pwma and log with your Archive Zimbra account. You can also **reset forgotten password** at the PWMA Portal if necessary **Important!** You need to have **mobile phone number registered at the portal** in advance to be able reset password via SMS.

Kerio Mailserver [K]

Use Kerio webmail (https://mbox.cerge-ei.cz/)

FACTS / HINTS

* **One account for all services** (called Domain Account). There is **only one login name and password** which serves **for** almost **all applications** and services at CERGE-EI (Login to computer; Network shares, CEIS; CMS; Reporting; internal web pages; printers etc.) Mostly the password is common also for Email Server Zimbra - including Webmail, SMTP and IMAP access; * You can have an **independent password for email** - coordinate accounts separation with the IT office in advance (older accounts are still synced between email and domain) * **Do not change the email password via Zimbra webmail** to make it independent, it could lock your network account. (Unless you are the person with the **independent email password**. This case use webmail for Zimbra Password change) * Password may be changed **ONLY ONCE per day**. * **Passwords must meet complexity requirements**

Please understand, that it is important to comply with the following rules: * Passwords must not contain the user's name or username; * Passwords must contain characters from the following four categories: uppercase characters,

lowercase characters, digits, other characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ * Must be at least 9 characters long.</WRAP> * **Passwords remembered by email clients can LOCK YOUR ACCOUNT * Account is temporarily locked after several unsuccessful logon attempts with a wrong password! * Email clients (like Thunderbird or Outlook), smartphones and tablets or web browsers (like Firefox or Chrome) allow password to be remembered. * BE AWARE that <font inherit/inherit;;red;;inherit>SMARTPHONES**<font inherit/inherit;;red;;inherit>**usually use remembered password repeatedly** regardless of its validity which results in the **account lockdown**.

- **Plan well before you change your password!** Recall all devices or applications with stored passwords (especially smartphones and tablets) in advance.
- **Immediately after the password change**, the client password in your mail, smartphone, tablet **must be changed too**.
- **What to do, if you find out that your AD account or mailbox is locked?**
- **Try to find the reason.** Have you made many unsuccessful attempts? Have you changed your password? Is your smartphone/tablet active?
- **Stop or power off any possible source of wrong passwords**, e.g. running mail client, browser, smartphone or tablet.
- **Wait a required timeperiod** (until automatic account unlock applies)
- **Check/change password settings in all client applications.** Mainly smartphones don't allow to change/save the new password without checking it on the server (It's impossible with locked account).
- **Email client usually requires both IMAP (incoming) and SMTP (outgoing) passwords to be set**

MORE DETAILED INFORMATION

Locking the account and mailbox

Account is temporarily locked after several unsuccessful logon attempts with wrong password to avoid abuse and brute force password breaking.
There are three significant parameters of this feature:

- permissible number of failed attempts;
- time window of fails;
- timeout of unlocking.

The account is locked if the number of allowed fails is exceeded. Failed attempts are counted during the time window. If logon attempts with wrong password stop, the counter is reset after the time window is over. If the account is locked, after the quarantine time it is unlocked again.

Special warning for smartphone users

Smartphones usually use remembered password repeatedly regardless of its validity. Than you can easily lock the mailbox unintentionally.

Threshold parameters - Active Directory

The Active Directory (shortly AD) serves as authentication authority for local network shares, desktop login, internal web pages, CEIS, CMS, Reporting etc.

Account lockout duration: **3 minutes**
Account lockout threshold: **7 invalid logon attempts**
Account lockout counter reset: **after 3 minutes**

Threshold parameters - Zimbra mailer

Number of consecutive failed logons allowed: **10**
Time to lockout the account: **30 minutes**
Time window in which the failed logons must occur to lock the account: **1 hour**

Although the AD account is locked earlier, it is also quickly unlocked. If the attack over the mailer persists, the lock on the mailer is activated for a longer period and produces no new lock of the AD account.

Links

More complex information is available in the User Accounts and Password usage article.