Enforcing Two-Factor Authentication at CERN

A Technical Report on Our Experiences with User Migration

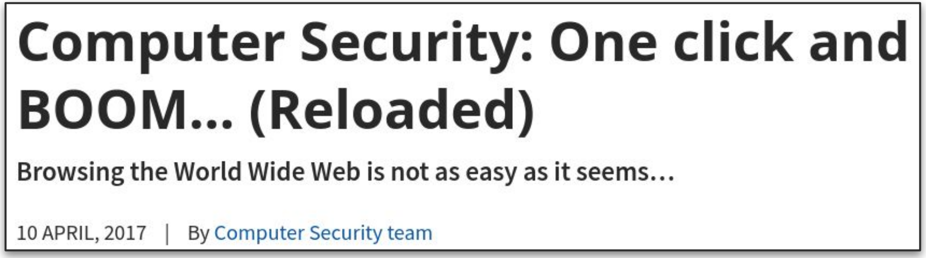
Combined effort from **CERN SSO & Computer Security Team**

Adeel Ahmad,
Asier Aguado Corman,
Hannah Short,
Liviu Valsan,
Maria Fava,
Sebastian Lopienski,
Stefan Lueders

Adeel Ahmad

Presented at ***CHEP, 2023***

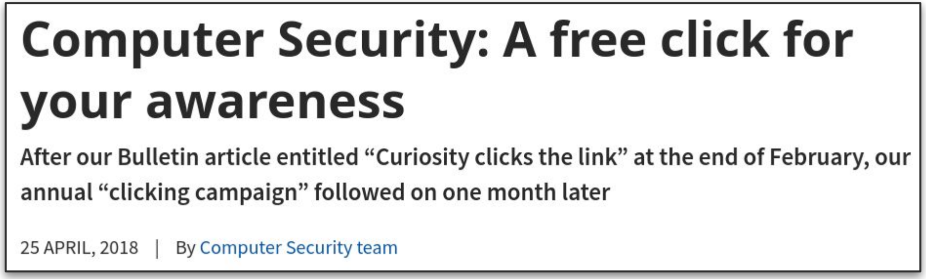
Raising User Awareness



Computer Security: One click and BOOM… (Reloaded)

Browsing the World Wide Web is not as easy as it seems…

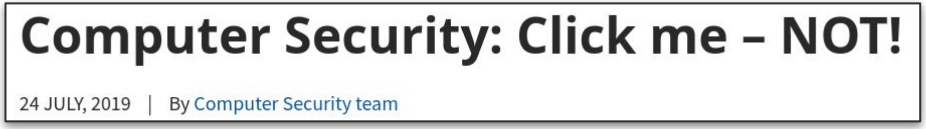
10 APRIL, 2017 | By Computer Security team



Computer Security: A free click for your awareness

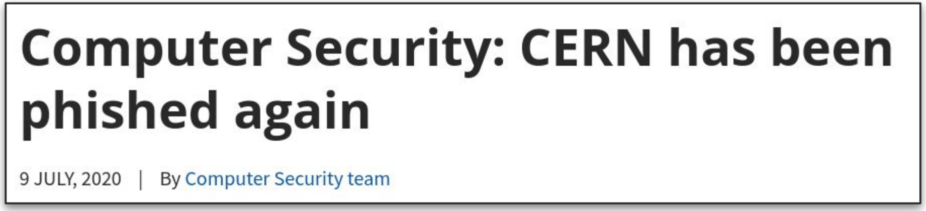
After our Bulletin article entitled “Curiosity clicks the link” at the end of February, our annual “clicking campaign” followed on one month later

25 APRIL, 2018 | By Computer Security team



Computer Security: Click me – NOT!

24 JULY, 2019 | By Computer Security team

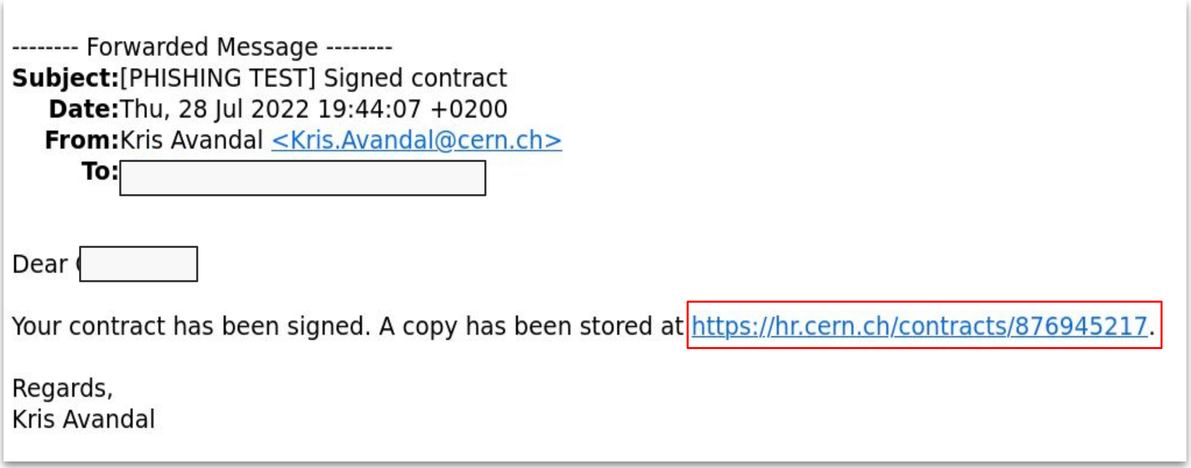


Computer Security: CERN has been phished again

9 JULY, 2020 | By Computer Security team

Phishing Campaigns

- Yearly campaign of **fake phishing emails** (22,731 total emails sent in 2022)
- **2000+ (9%)** users gave away their credentials
  - **(No actual data was compromised)**

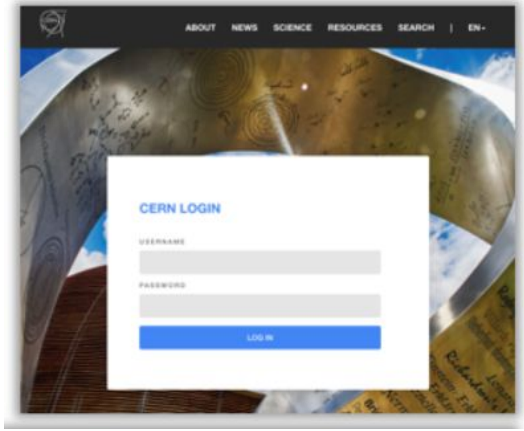


-------- Forwarded Message --------
Subject:[PHISHING TEST] Signed contract
Date: Thu, 28 Jul 2022 19:44:07 +0200
From: Kris Avandal <Kris.Avandal@cern.ch>
To:[redacted]

Dear [redacted]

Your contract has been signed. A copy has been stored at https://hr.cern.ch/contracts/876945217.

Regards,
Kris Avandal



The Onset…

Computer Security: Multifactor for the masses

News | Computing | 11 November, 2021

[...] in 2022, we would like to take the next step: using two-factor authentication when logging into any CERN [...] application.

https://home.cern/news/news/computing/computer-security-multifactor-masses

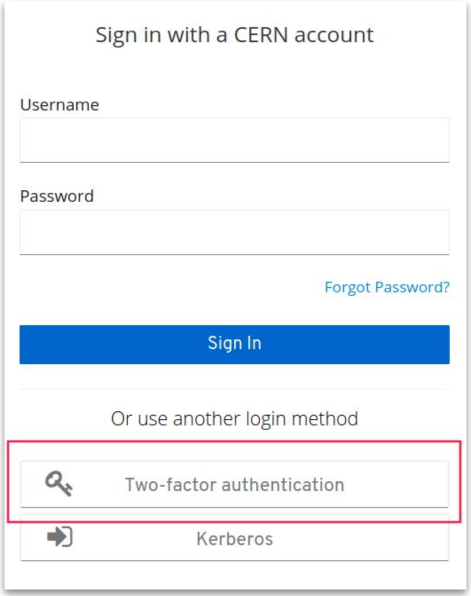
Pre-2022 Login Flow

Using Keycloak as our SSO solution

- Login possible via Kerberos or username / password

2FA was enabled optionally as a separate login

- The login flow was **cumbersome**
- Users had to **logout & re-authenticate** to access a 2FA application



Sign in with a CERN account

Username

Password

Forgot Password?

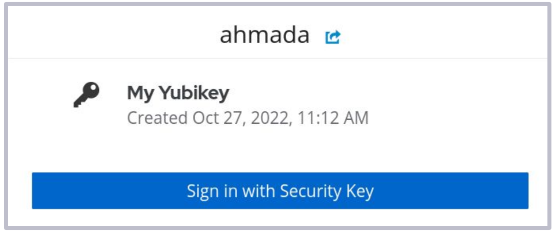
Sign In

Or use another login method

Two-factor authentication

Kerberos

(Keycloak Login Page)



ahmada

My Yubikey
Created Oct 27, 2022, 11:12 AM

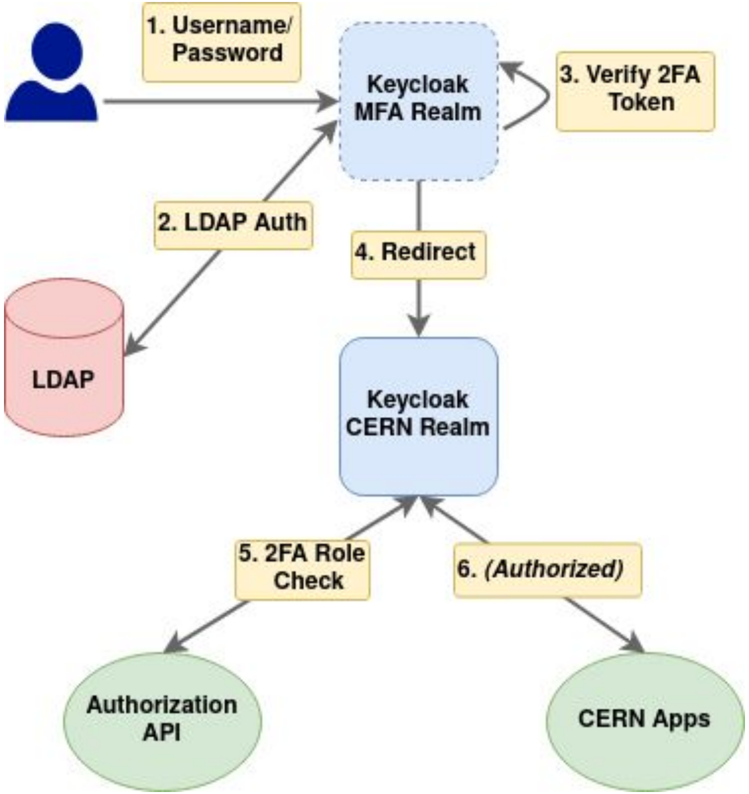
Sign in with Security Key

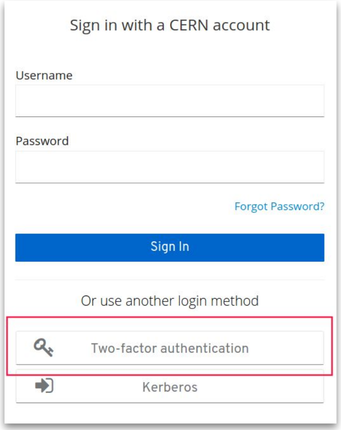
(2FA Prompt)

Complex Keycloak Configuration

- **Inefficient two-realm setup** (user data duplicated)
  - **Non-2FA** authentication: **cern realm**
  - **2FA** authentication: **mfa realm**
- **Custom code** for identifying if user logged in with 2FA

Old Login Flow





Sign in with a CERN account

Username

Password

Forgot Password?

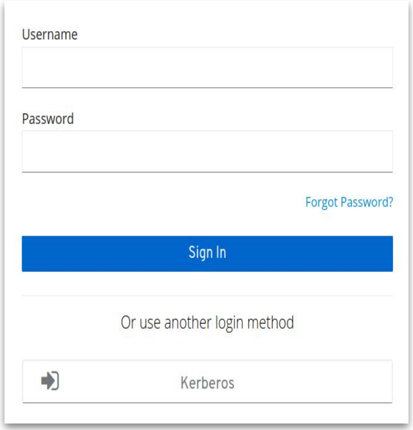
Sign In

Or use another login method

Two-factor authentication

Kerberos

(Main login page)



Username

Password

Forgot Password?

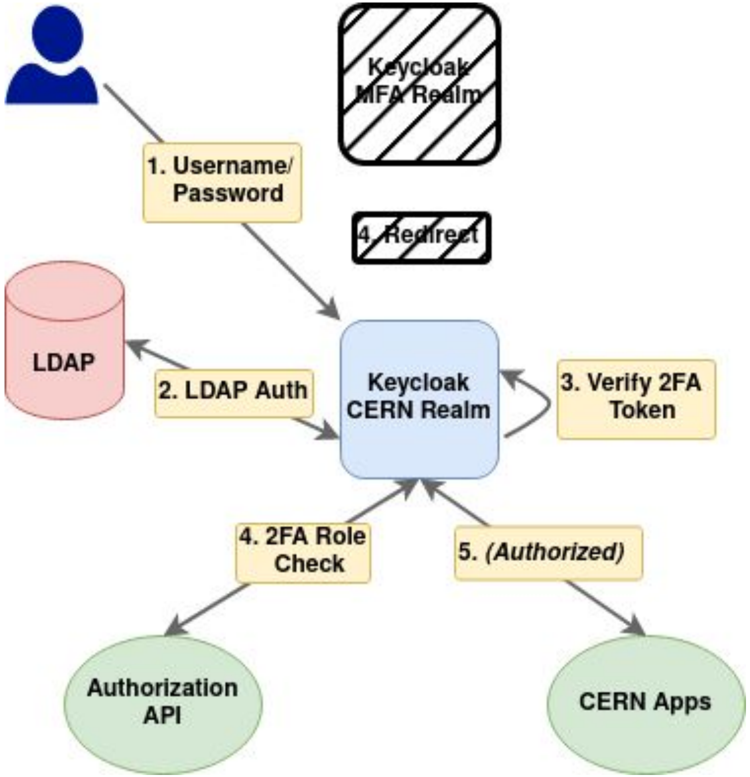
Sign In

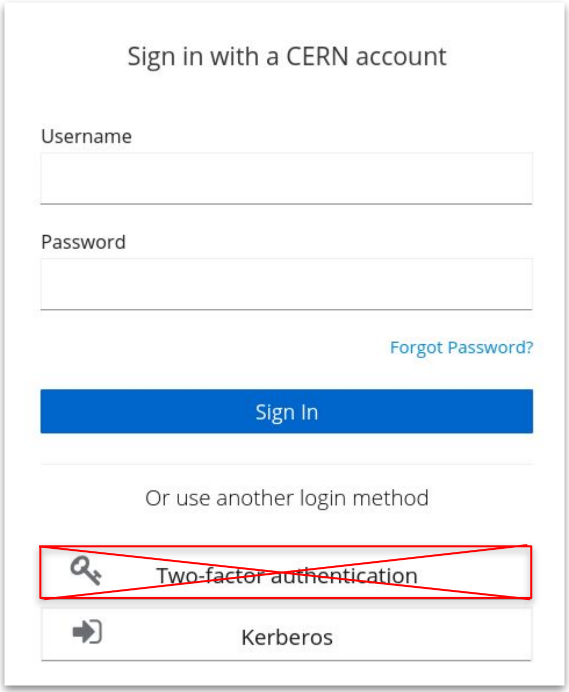
Or use another login method

Kerberos

(2FA login page)

Desired Future Login Flow





Sign in with a CERN account

Username

Password

Forgot Password?

Sign In

Or use another login method

~~Two-factor authentication~~

Kerberos

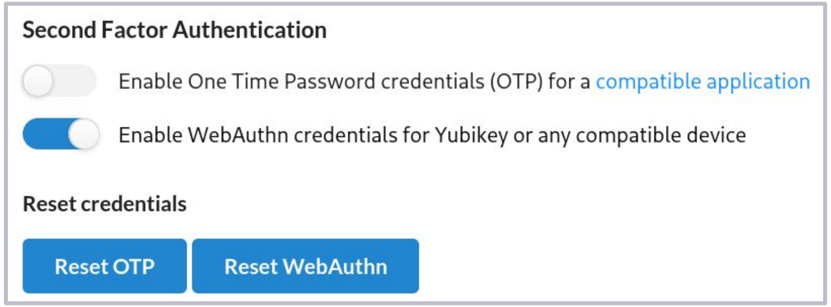
(Simpler Login Screen)

Shortcomings of Old Approach

- Optional 2FA **protects applications**, but **not accounts**
- Not all critical applications (e.g. Email) required 2FA, meaning a **compromised account** could still do significant damage

New Approach

- 2FA is either enabled or disabled for the account, i.e. ***Always-on*** *or* ***Always-off***
- **Voluntary users** can **opt-in** and **opt-out** at will
  - 2FA mandatory if users want to access an application requiring 2FA
- Security team maintains a group of **critical users** who **must** use 2FA



Second Factor Authentication

○ Enable One Time Password credentials (OTP) for a compatible application

● Enable WebAuthn credentials for Yubikey or any compatible device

Reset credentials

Supported 2FA Methods

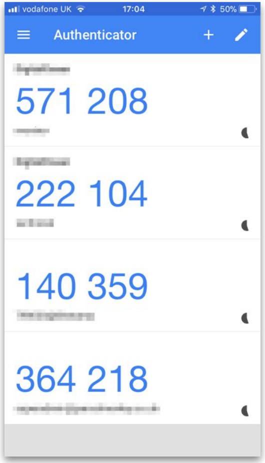
WebAuthn (Yubikey, fingerprint readers, e.g. Macbook)

(USB-A, USB-C, NFC)

1419 Enabled Accounts

One Time Password (OTP)

Google Authenticator, Aegis Authenticator, Raivo OTP, Hardware TOTP devices (Token2)



vodafone UK 17:04 50%

Authenticator

571 208

222 104

140 359

364 218

Migration Workflow

- Users to be migrated are added in a **Group**
- **Migration script** runs hourly
  - Copies user's 2FA tokens to the new realm in Keycloak
  - Flags user account to make 2FA mandatory
- Users are in **three states**: **2FA migrated**, **2FA non-migrated**, **no-2FA**

Shortcomings of Mid-Transition Phase

- **Slow** synchronization of groups
- Have to keep **both systems** running in parallel

Impact on Users

- Relatively **low number of serious complaints** where people were unable (or seriously impacted) to work

- 2FA for **mobile** use seen as particularly difficult
  - **Browser sessions** do not remain active, as browser app gets killed (limitation of mobile OS)
    - Bypass list to skip 2FA login

- WebAuthn doesn't work on **Remote Desktops** (requires configuration)

- Some **CLI tools unusable** (using password grant)

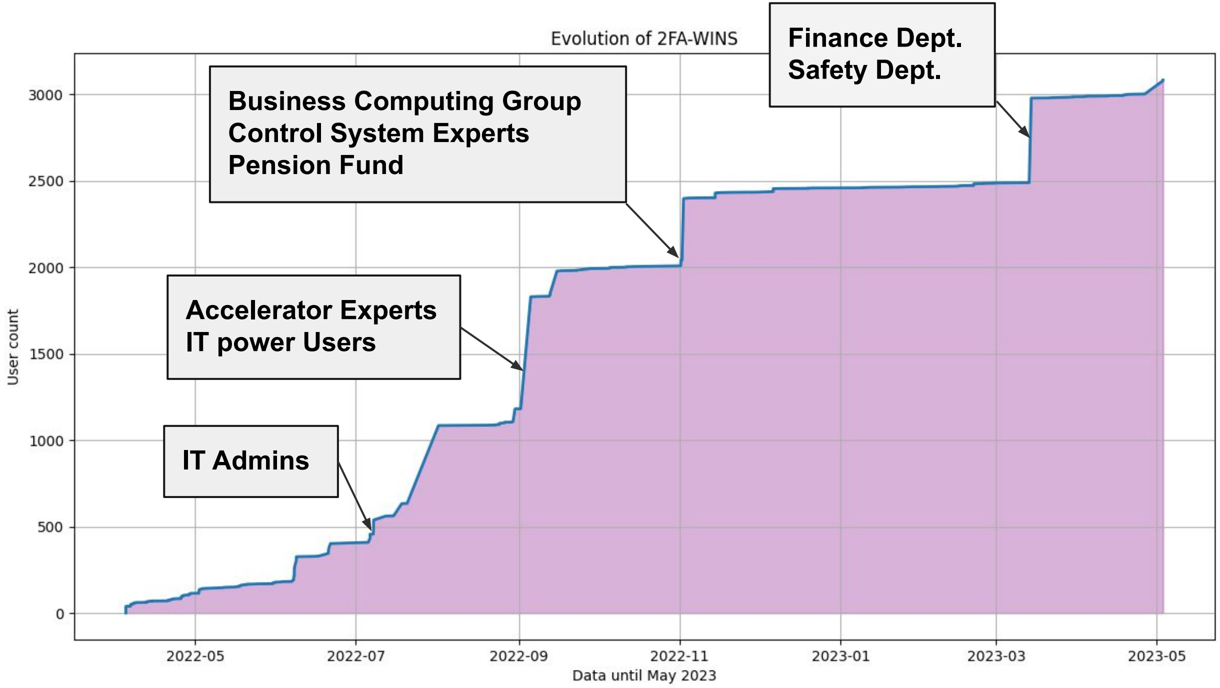
2FA Feedback and Improvements

- **Push notifications**; not possible natively with current Keycloak version
- **Persistent Cookies** for sticky 12 hour sessions between browser restarts (already released)
- **Multiple 2FA tokens of the same type** (work planned)

Additional Security Improvements

- **Compromised passwords check** using "Have I Been Pwned" database
    - Annual password change no longer required

Migration Timeline - ~2500 users migrated



IT Admins

Accelerator Experts
IT power Users

Business Computing Group
Control System Experts
Pension Fund

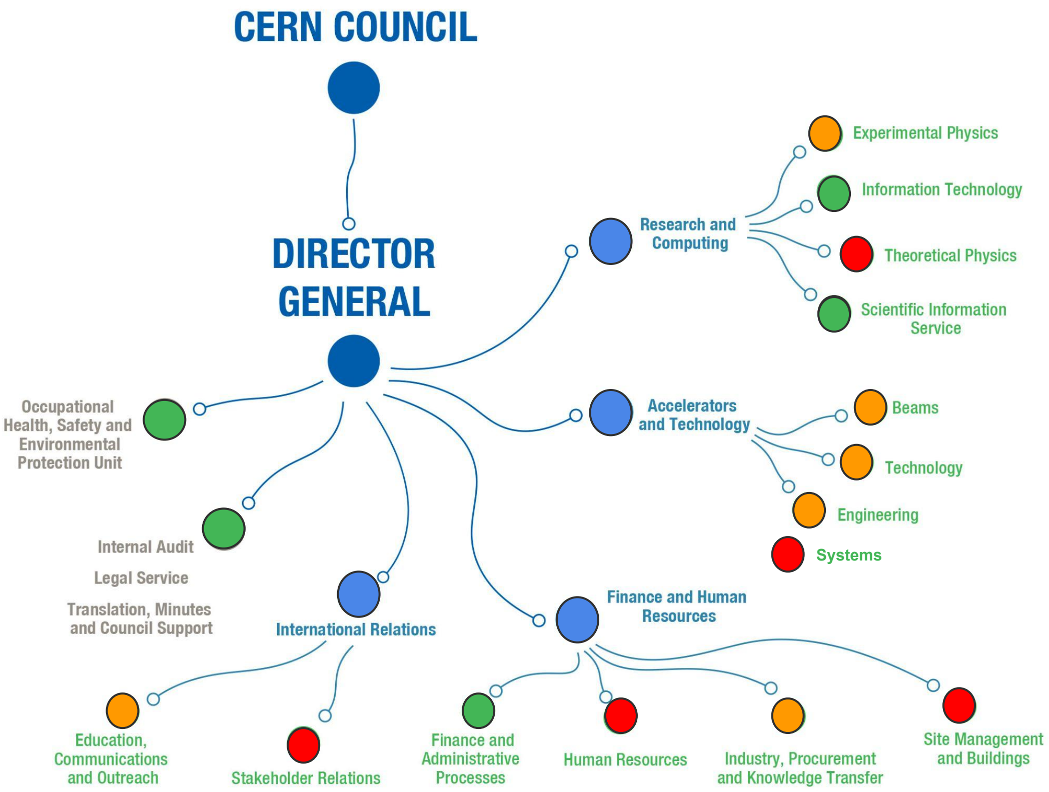
Finance Dept.
Safety Dept.

Migration Chart

🟢 Migrated

🟠 Partially migrated

🔴 Not migrated


CERN COUNCIL
DIRECTOR GENERAL
Research and Computing
Experimental Physics
Information Technology
Theoretical Physics
Scientific Information Service
Accelerators and Technology
Beams
Technology
Engineering
Systems
Occupational Health, Safety and Environmental Protection Unit
Internal Audit
Legal Service
Translation, Minutes and Council Support
International Relations
Education, Communications and Outreach
Stakeholder Relations
Finance and Human Resources
Finance and Administrative Processes
Human Resources
Industry, Procurement and Knowledge Transfer
Site Management and Buildings

Next Steps

- **Complete transition** to Always-On 2FA (i.e. a single realm in Keycloak)
- Work on **usability features** e.g. multiple MFA tokens
- Add support for **step-up authentication**

Want more information?

Visit auth.docs.cern.ch