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,
Stefan Lueders

Adeel Ahmad

Presented at HEPiX, 2022
Background

CERN is transitioning to a new SSO (Keycloak)
• Good opportunity to adopt 2FA, well supported by Keycloak

In the past 2FA was enabled optionally as a separate login
• The login flow was cumbersome
• Applications had to specifically require 2FA
Motivation (I) - Many users don't use 2FA

Results of Phishing Campaign

- Yearly campaign of fake phishing emails (22,731 total emails sent)
- 2000+ (10%) 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: [blank]

Dear [blank]

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

Regards,
Kris Avandal
Motivation (II) - Complicated workflow

- Required **logout & re-authentication** to access 2FA enabled websites

- Applications could require authentication via 2FA but flow was **cumbersome**, e.g. below.

Unauthorized to log in. This application requires two-factor authentication. Please log out, and then log in again using a two-factor authentication method.

« Log out and go back to Application
Motivation (III) - Inefficiencies in current system

Simplification of Keycloak Configuration

- **Two-realm setup** (each connects to Active Directory)
  - Non-2FA authentication: cern
  - 2FA authentication: mfa

- User data is *duplicated* in both realms
Motivation (III) - Old Flow (Cont.)

1. Username/Password
2. LDAP Auth
3. Verify 2FA Token
4. Redirect
5. 2FA Role Check
6. (Authorized)

LDAP

Keycloak MFA Realm

Keycloak CERN Realm

Authorization API

CERN Apps

Sign in with a CERN account
Username
Password

Sign In

Or use another login method
Two-factor authentication
Kerberos

UserName
Password

Sign In

Or use another login method
Two-factor authentication
Kerberos

(Main login page)

(2FA login page)
Enforcing Two-Factor Authentication at CERN
Shortcomings of Old Approach

- Optional 2FA protects applications, but not accounts
- Not all critical applications required 2FA meaning that 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 they want to access an application that requires 2FA

- Security maintains a group of **critical users** who **must** use 2FA
Supported 2FA Methods

**WebAuthn (Yubikey)**
(USB-A, USB-C, NFC)
1419 registered Yubikeys (404 used for SSH)

**One Time Password (OTP)**
Google Authenticator, Aegis Authenticator, Raivo OTP
Migration Workflow (I)

- **E-group** (maintained by Security) contains migrated users
- **Migration script** runs hourly
  - Copies user's 2FA tokens to the new realm in Keycloak
  - Adds migrated role in Keycloak
- Users are in **three states**: 2FA migrated, 2FA non-migrated, no-2FA
Migration Workflow (II)

2FA for SSH (in progress)

● Pluggable authentication module (PAM) still references the **old "mfa" realm**

● **Script** to synchronize 2FA credentials between both realms

```bash
$ ssh ahmada@aiadm.cern.ch
(ahmada@aiadm.cern.ch) Your 2nd factor (ahmada):

SSH'ing into a 2FA-protected machine
```
Shortcomings of Mid-Transition Phase

- **Slow** E-groups to Grappa synchronization
- SSH users **cannot login** during migration
- Have to keep **both systems** running in parallel
Impact on Users

- Some unhappy users but relatively low number of complaints (~20)
- 2FA for mobile use seen as particularly difficult
  - Browser sessions do not remain active, as browser app gets killed (limitation of mobile OS)
- WebAuthn doesn't work on RDP clients (unsupported)
2FA Feedback and Improvements

- Much feedback gathered through internal channels - thank you!
  - Some requests not possible with Keycloak, e.g. push notifications

- Persistent Cookies for sticky 12 hour sessions between browser restarts (work in progress)

- Multiple 2FA tokens (work planned)

- Reset procedure too long (new procedure for remote ID vetting)
Additional Security Improvements

- **Compromised passwords check** using HIBP database
  - Annual password change no longer required
- **Rate-limiting** per IP address (Nginx and HAProxy)
Migration Timeline - ~1600 users migrated
Next Steps

- **Complete transition** to Always-On 2FA (i.e. a single realm in Keycloak)
- Work on **usability features** e.g. multiple MFA tokens
Want more information?

Visit auth.docs.cern.ch