

The Second-Factor Authentication System at CERN

Adeel Ahmad^{1,*}, *Asier Aguado Corman*¹, *Hannah Short*^{1,**}, *Liviu Valsan*¹, *Maria Fava*¹, *Paolo Tedesco*¹, *Sebastian Lopienski*¹, *Stefan Lueders*¹, and *Vincent Brillault*¹

¹European Organization for Nuclear Research (CERN)

Abstract.

In 2022, CERN ran its annual simulated phishing campaign in which 2000 users gave away their passwords. In a real phishing incident, this would have meant 2000 compromised accounts, unless they were protected by Two-Factor Authentication (2FA). In the same year, CERN introduced 2FA for accounts with access to critical services. The new login flow requires users to always authenticate with a 2FA token, either with Time-based one-time password (TOTP) or WebAuthn. This introduces a significant security improvement for the individual and for the laboratory. The previous flow enforced 2FA to access a small number of applications. In this paper, we will discuss the rationale behind the 2FA deployment, as well as the technical setup of 2FA in the CERN Single Sign-On system, Keycloak. The paper will give a detailed overview of the architecture for this new 2FA flow and compare how it differs from the legacy 2FA system which was in place since 2019. We share statistics on how users are responding to this change in the login flow, and the actions we have taken to improve the user experience. Finally, we briefly describe our custom extensions to Keycloak for specific use cases, which include adding roles in the user token, overriding the default Keycloak session, and modifying the user login flow.

1 Introduction

During 2022, the European Organisation for Nuclear Research (CERN) introduced permanent Two-Factor Authentication (2FA) for accounts that have access to critical services, which include OpenStack and Judy (a service used for provisioning Puppet-managed VMs). The new flow requires users to always authenticate with a 2FA token, using either the TOTP or WebAuthn protocol. In this paper, we will discuss the rationale behind the 2FA deployment, as well as the technical setup of 2FA in CERN's Single Sign-On. All technical discussion will be related with Keycloak ¹, which is the SSO software used at CERN. The paper will present an overview of the legacy 2FA system which is being replaced with a newer system. The new system is more efficient and robust. We next delve deep into the technical setup of this system and explain how we are migrating users from the old to the new system. Then, we present the migration strategy adopted at CERN and statistics on how many people have adopted the new 2FA.

*e-mail: adeel.ahmad@cern.ch

**e-mail: hannah.short@cern.ch

¹<https://www.keycloak.org/>

1.1 Legacy 2FA System

CERN introduced Two-Factor Authentication (2FA) in its login flow in 2019. Initially, it was not enforced for all users, but rather application owners had the ability to make it mandatory for accessing their application. Due to this, many users never opted in for 2FA unless they needed to access an application which required 2FA. Another drawback of this optional 2FA approach was that it required creating a separate realm within Keycloak, thus duplicating all users, which added an overhead on the software. This flow allowed users to login with 2FA using a dedicated option in the SSO login portal, shown in Figure 1. The main users of this login flow consisted of the IT department which offered certain critical applications. These applications had a role set in their Keycloak configuration which made it mandatory for users to login with 2FA.

Sign in with a CERN account

Username

Password

[Forgot Password?](#)

Or use another login method

-
-

Figure 1. Optional (legacy) 2FA login button in the CERN SSO login page.

The legacy 2FA login flow which was in use until recently is shown in Figure 2.

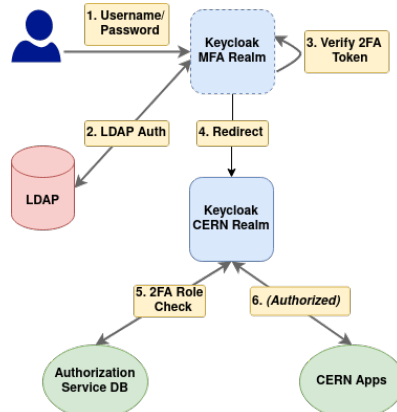


Figure 2. Old 2FA login flow using a separate “mfa” realm for 2FA.

2 Always-on 2FA

In late 2020, the CERN Computer Security team took a mandate ² to make 2FA mandatory and couple it with the user account. This new flow requires users to provide their 2FA token for each login, if enabled for their account. In addition to improving security, since the account became protected for all SSO access, this solved two main problems:

- Users were no longer required to re-login when they wanted to access a 2FA-protected application.
- The complex Keycloak setup and login flow could be simplified.

The new 2FA flow is tied to the user's account rather than with the end application in a single realm. A realm in Keycloak is a space which includes users, applications, roles, and groups. We now provide 2FA from the "cern" realm in Keycloak, contrary to the 2FA provided in "mfa" realm, as done previously. A migration script, "migrate-users-2fa", is responsible for migrating users from the old to the new 2FA flow. The new login flow setup for 2FA is shown in Figure 3. The source files for these diagrams are available on CERNBox.

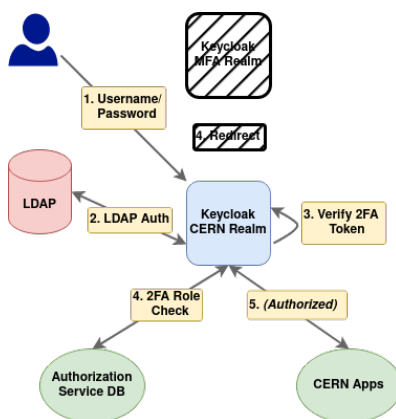


Figure 3. New 2FA login flow providing 2FA and 1FA logins from a single "cern" realm.

3 Keycloak Configuration

We introduced several customizations in Keycloak, as previously mentioned. These features were provided by implementing the Keycloak Service Providers (SPIs) which were written in Java to add a custom role in the user token if they logged in with 2FA. Furthermore, we changed the default Keycloak authentication flow to check for a specific role in the user profile and to prompt them for a 2FA token, if present. This login flow also included a check for the user password reset flag in our database and to display a form to reset the user password.

3.1 Custom Extensions (SPIs)

Keycloak allows modifying the default authentication flow to add a custom check and verification before the user logs in. In our custom 2FA login flow, we check if the user has the 2FA

²<https://home.cern/news/news/computing/computer-security-multifactor-masses>

migrated role present in their profile. The 2FA login screen is only presented if this role is already present. Other SPIs that we have developed include adding a custom role in the user token and checking if the user password has been compromised.

In the old login flow (Figure 1), 2FA login is provided using a separate button which redirects users to login using a different login screen. The new system incorporates 2FA and 1FA logins within the same login flow.

Note that in Figure 4 there is the addition of “2FA Migrated Role” which indicates whether a user is using the new 2FA flow or not. This is a temporary solution which allows both optional and Always-on 2FA systems to co-exist while we run the migration campaign.

Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy CIBA Policy

Browser 2FA - Skip Migrated Users		Requirement	New	Copy	Delete	Edit Flow	Add execution	Add flow
Auth Type	Cookie	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED				Actions
	Identity Provider Redirector	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input checked="" type="radio"/> DISABLED				Actions
	Browser 2FA - Skip Migrated Users Forms	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		<input type="radio"/> CONDITIONAL		Actions
	Username Password Form	<input checked="" type="radio"/> REQUIRED						Actions
	Browser 2FA - Skip Migrated Users Second Factor	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		<input checked="" type="radio"/> CONDITIONAL		Actions
	Condition - User Configured	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED					Actions
	Condition - User Role (2fa-not-migrated)	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED					Actions
	OTP Form	<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED				Actions
	WebAuthn Authenticator	<input type="radio"/> REQUIRED	<input checked="" type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED				Actions
	Browser 2FA - Skip Migrated Users Force Password Reset	<input type="radio"/> REQUIRED	<input type="radio"/> ALTERNATIVE	<input type="radio"/> DISABLED		<input checked="" type="radio"/> CONDITIONAL		Actions
	Condition - Reset Password if Authn Required	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED					Actions
	CERN Reset Password Form	<input checked="" type="radio"/> REQUIRED	<input type="radio"/> DISABLED					Actions

Figure 4. 2FA Login Flow MFA

3.2 Role Check

The role check in Keycloak is done within the login flow. This role is added to the user profile in both the “cern” and “mfa” realms. We make use of a 2FA CLI command to add this role to the user.

4 Migration Strategy

The CERN Computer Security team started rolling out the new 2FA in February 2021. Initially, users from the IT department were migrated to the new flow and were asked for their feedback. Gradually, we asked for volunteers from other departments to opt-in to the Always-on 2FA flow. We currently have around 3,000 users in the new 2FA flow, while the total user count is above 10,000. However, the majority of unmigrated users are externally affiliated university employees at CERN and can be migrated at once. The Computer Security team also maintains a list of critical accounts which are obliged to use 2FA, and, hence, do not have the ability to opt out (i.e. disable both their 2FA tokens). The migration is controlled using an internal group which is open to subscription from any CERN account. A migration script is responsible for reading users from this group and 1) adding the required roles in their Keycloak profile and 2) copying their 2FA tokens from the old to the new realm. The chart in Figure 5 shows a detailed overview of migrated users in Keycloak.

The diagram in Figure 6 shows which departments are fully migrated, partially migrated, or pending migration.

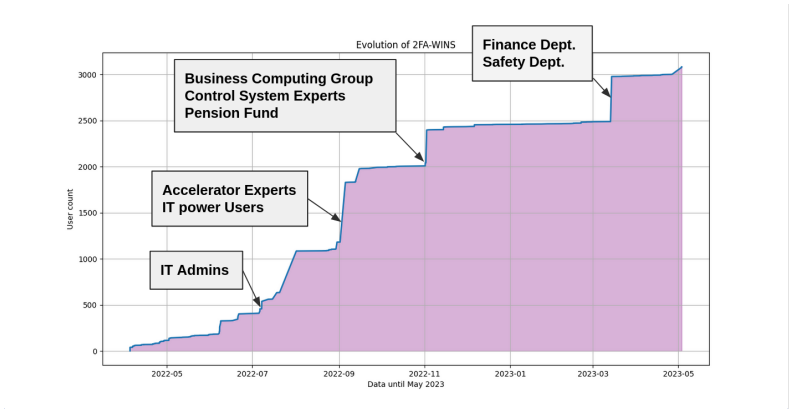


Figure 5. 2FA Migration Timeline

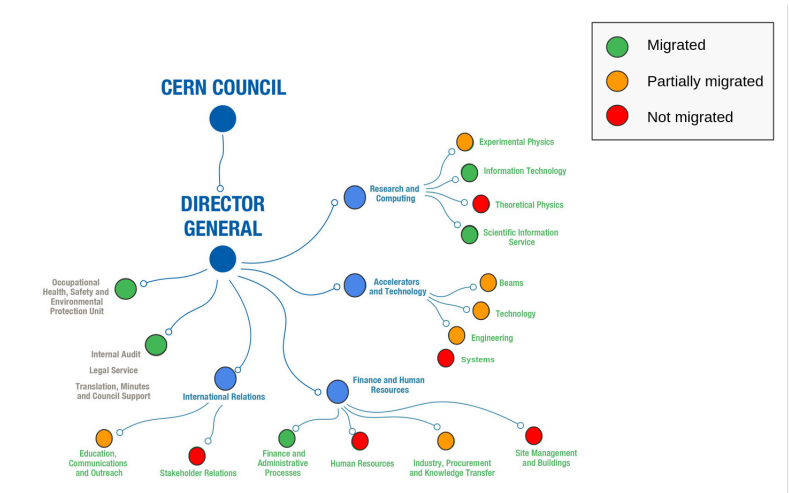


Figure 6. 2FA Migration Diagram

4.1 Command-Line Interface tool

The authentication team has developed a Python CLI tool to help with migrating users and to generate statistics on the migration phase. This tool runs as a cron job to periodically synchronize users in the 2FA group and adds the migrated role to their Keycloak profile. We currently have the following cron jobs in place:

- “migrate-users-2fa”: Moves users to the new 2FA flow and copies their 2FA credentials.
- “remove-users-from-mfa-role”: Removes users from the new 2FA flow who are in the bypass list.
- “get-users-2fa”: Returns a list of (un)migrated users to the new 2FA flow.

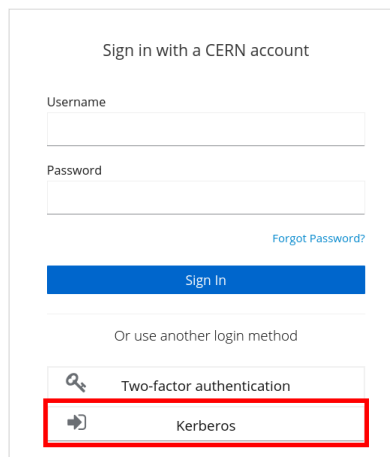
This tool is also installed on a virtual machine which is accessible by the CERN Computer Security team to run their own statistics.

4.2 Critical Users

The Computer Security team has defined a list of critical users who are obliged to use 2FA for each login. These users do not have the ability to disable both their 2FA methods. This is made possible by adding these users to a special authorization group. In the API, we check if the user is part of this authorization group and deny their request to disable both their 2FA methods.

4.3 Kerberos Configuration

To simplify SSO access we also offer logins with Kerberos. All CERN-managed Windows machines get a valid Kerberos ticket on login and can login without re-entering their username and password. We provide Kerberos logins using a separate Identity Provider in both the “cern” and “mfa” realm. The reason to create a separate IDP is to avoid automatic logins if the user already has a valid Kerberos ticket present. With this flow, users can choose to authenticate with Kerberos by pressing a separate button on the SSO login page, as shown in Figure 7.



The image shows a login interface titled "Sign in with a CERN account". It contains two input fields for "Username" and "Password", with a "Forgot Password?" link below the password field. A blue "Sign In" button is positioned below the password field. Below this, the text "Or use another login method" is displayed. Underneath, there are two options: "Two-factor authentication" (with a key icon) and "Kerberos" (with a key icon). The "Kerberos" option is highlighted with a red rectangular border.

Figure 7. Kerberos login.

4.4 Guest and Social Logins

Both Guest and Social logins remain unaffected by this change as these accounts do not have the ability to enable 2FA. These accounts only have access to a limited number of services and thus are not deemed critical. Guest accounts refer to externally registered users in the Keycloak database and Social accounts consist of externally federated logins from Google, Facebook, etc.

5 Conclusions & Next Steps

We plan to finish the 2FA migration in Q4 2023 and remove all logic relating to the optional 2FA flow. There have been numerous requests from users to add new features to our system;

these include the ability to register multiple 2FA tokens and add support for step-up authentication for applications requiring 2FA. These features are now natively supported in newer versions of Keycloak and thus will be made available to our users. The timeline for providing this new functionality has yet to be determined.

Useful resources are included in Appendix A.

References

A Resources

- User documentation for the CERN authorization Service: <https://auth.docs.cern.ch>
- Keycloak documentation: <https://www.keycloak.org/documentation>