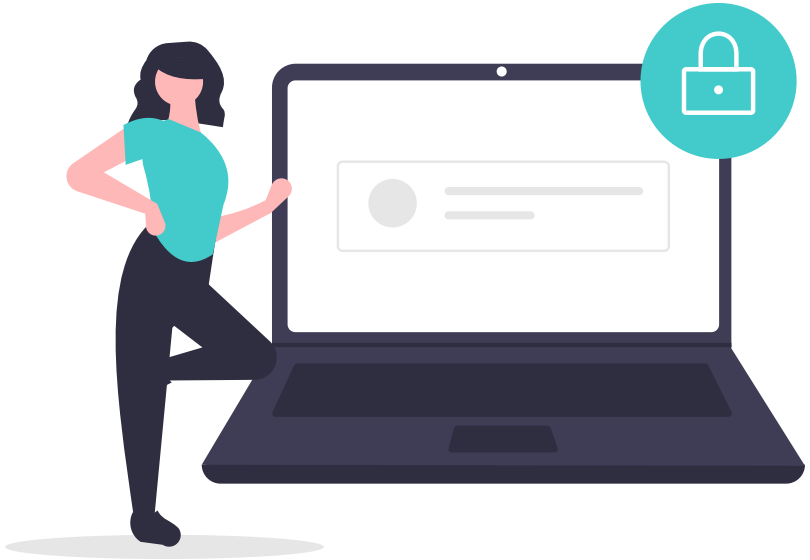
DHIS2 Security Features

Michael Markevich, DHIS2 Security Lead

DHIS2 Annual Conference 2023
Oslo, Norway



DHIS2 Security Features

dhis2

Access Control

- Core functionality
- Users can belong to groups and can have role assignments
- Roles contain fine-grained authorities
- Users can have restrictions based on the analytics dimension

LDAP Authentication

- Core functionality
- Active Directory, Azure AD, OpenLDAP, or compatible service supported

Multi-Factor Authentication

- Available in DHIS2 2.30+
- Based on Google Authenticator or any other compatible application for smartphones or feature phones

Single Sign-On

- Available in DHIS2 2.35+
- We support OpenId Connect (OIDC), which is compatible with popular identity management systems like Okta, Keycloak, etc.

Personal Access Tokens

- Available in DHIS2 2.37+
- Personal access tokens are an alternative to using password-based authentication for automation using API calls

User Impersonation

- Available in DHIS2 2.40+
- Using a special privilege, DHIS2 administrators can impersonate other users and execute commands on their behalf (similar to `sudo` in Linux).

dhis2

Auditing and Logging

- Core functionality
- User activity log
- System event log

Backup

- Data backup applies to the DHIS2 database (PostgreSQL)
- It can be configured with external tools outside of the DHIS2 instance

Virtual Patching

If you run a DHIS2 instance behind Nginx in a reverse proxy mode, we can provide configuration snippets to mitigate known security vulnerabilities or protect against selected attacks.

Security Team Updates

Reference Setup

We have created a reference setup of DHIS2, which can be used for public penetration testing of our recommended security configuration.

Security Hall of Fame

We have created the Security Hall of Fame page, acknowledging contributions from independent security researchers.

We also plan to promote our security program publicly and attract more experts to evaluate the security of DHIS2.

dhis2

Thank You