

— IDENTITY DEDUPLICATION AND IDENTITY MANAGEMENT (SAML 2.0 SINGLE SIGN-ON)

Kimlock

One identity, one username and one sign-on per person

Kimlock is identity management software that takes records from student information systems, HR and personnel systems and other source systems and consolidates each person into a single identity keyed by their national ID number. A person's different roles are kept as separate accounts under one user; accounts are provisioned in OpenLDAP, Active Directory, Zimbra and Google Workspace. Users sign in once over SAML 2.0 to Microsoft 365 / Entra ID, Google Workspace and services in the eduGAIN federation, and use the same identity for Wi-Fi and VPN over RADIUS; sign-ins can be protected with multi-factor authentication by SMS, email or an authenticator app. Password tasks are self-service, verified by SMS or email code.

HIGHLIGHTS

01

One identity per person

Student and staff records from different sources are matched by national ID number; each role is kept as a separate account, with its registry number, type and unit, under one user.

02

SAML 2.0 single sign-on and federation

The identity provider offers single sign-on and sign-out to Microsoft 365 / Entra ID, Google Workspace and services in the eduGAIN federation. Wi-Fi and VPN logins are authenticated with the same identity over RADIUS.

03

Automatic flow from source to directory

Records from the student information system and the HR/personnel system are imported through field mapping; accounts are opened, updated and closed in OpenLDAP, Active Directory, Zimbra and Google Workspace.

04

Self-service password and account recovery

Changing a password, resetting a forgotten one and recovering a username are done with a code sent by SMS or email, without the help desk.

WHO IT'S FOR

Universities where one person can be both a student and a staff member

Organisations whose personal data is spread across several systems and that want one identity record

IT departments that want OpenLDAP and Zimbra accounts opened and closed automatically from the source system

Organisations that want one username and password for SAML-enabled applications

Help desks moving password reset requests to self-service

Universities that want one identity for Microsoft 365, Google Workspace and eduGAIN services

Features 92 FEATURES

The list below shows, module by module, what the current version of the product does.

Identity records 6

- Individual and legal-entity identity types
- Unique record by identity type and number
- Multiple phone numbers (mobile, work, home etc.) and email addresses
- Identity photo
- Change history with old and new values
- Listing, search and Excel export

Users and accounts 8

- One user per identity; a separate account record per role
- User types in a tree (staff, student etc.)
- User tags
- Active, passive, semi-passive, blocked and provisioning states
- Passive, deleted and manually opened account lists
- Username suggestions from name and surname; blacklist of inappropriate words
- Email alias and forwarding records
- Admin password assignment: manual or policy-compliant auto-generated, delivered by SMS

Deduplication and data import 9

- Integration with student information systems and HR/personnel systems
- Import of student, staff and unit records from REST sources
- Merging source records into one identity by national ID number
- No-code field mapping, fixing and default value rules
- Numerator for records without a registry number
- Only changed fields are updated
- Lists of duplicate and deleted source records
- Import logs and user type breakdown
- Automating identity processes with transfer and mapping rules defined without code

Units 5

- Units and unit types in a tree

- Unit names in Turkish and English
- Listing users by unit
- Default directory settings per unit
- Updating the YÖKSİS unit structure from Excel

Single sign-on (IdP) 13

- SAML 2.0 single sign-on and single logout
- Second-step sign-in verification with an SMS or email code
- Multi-factor authentication with an authenticator app (TOTP)
- Artifact resolution service
- Viewing and downloading IdP metadata
- Adding service providers by metadata, enabling and disabling them
- Login name by user type: email, national ID, student number
- Post-login redirect by user type
- Per-domain settings; logo and login page background
- SAML 2.0 federation with Microsoft 365 / Entra ID
- SAML 2.0 single sign-on to Google Workspace
- Sign-in to eduGAIN federation services via the national federation
- Wi-Fi and VPN authentication over RADIUS

Self-service portal 7

- Password change
- Forgotten password reset
- Forgot my username: with ID number and configurable verification fields
- Verification code by SMS or email; time limit and three attempts
- reCAPTCHA after failed attempts
- Password rules shown in the interface
- Turkish and English interface

Directory and email integrations 13

- OpenLDAP server definition and connection test
- Create, update and delete users in OpenLDAP

- Units created as OUs in OpenLDAP
- LDAP attribute mapping per user type
- Reading an existing LDAP tree
- Zimbra server definition; create, update and close mail accounts
- Changed users synchronised by a background service
- Active Directory user and OU provisioning
- Google Workspace user and mailbox provisioning
- Directory integration with Azure AD / Entra ID
- Bulk and automatic user creation and group management in connected directories
- Password changes propagated to connected directories
- Matching with accounts in other applications

Mail groups 6

- Managing Google Workspace and Zimbra mail groups from one interface
- Mail group definitions per domain
- Membership from units, user types and tags
- Adding individual members and excluding users
- Activating and deactivating members
- Excel export of the group list

SMS and email 5

- Net GSM, Turatel and Sanal Santral SMS accounts; connection test
- SMTP email accounts and priority order
- Per-language editing of verification and notification texts
- Bulk SMS lists and sending
- Verification codes and passwords masked in SMS and email logs

API access 7

- Username and password verification endpoint
- Unit query and insert endpoint
- Endpoints for student, staff and password operations from the source system
- API accounts restricted by IP address
- API account scope: users, units, user types and tags
- API call logs
- API authorisation by application, user type and group membership

Access control and reports 6

- IP allow-list for the identity provider and admin panel
- Session and event logs
- User action log: verification, password change and reset
- Administrator action log
- User activity and error log reports
- Dashboard: user type counts and breakdown

Settings and policies 7

- Domains
- Role definitions and permission tree
- Admin panel users, activation and deactivation
- Password policy per user type
- Verification code policy per user type
- Terms of use and document texts
- Logo and login page background

Technical specifications

Foundation	The SAML layer is built on open-source SimpleSAMLphp; the applications use Phalcon 4 (PHP 7.x), the database is PostgreSQL and the interfaces are React. The identity model, data import, admin panel and integrations are product-specific
Identity matching	Identity type and number (national ID) as unique key; one user per identity and one account record per role
Protocols	SAML 2.0 identity provider (SSO, SLO, artifact resolution); RADIUS; JSON REST API
Multi-factor authentication	SMS or email verification code; time-based one-time code (TOTP) with an authenticator app
Data import	Student information system, HR/personnel system and other REST sources; configurable field mapping; add/update/delete by change comparison
Directory and email	User, OU and group provisioning in OpenLDAP, Active Directory and Azure AD / Entra ID; mailbox and group management via Zimbra SOAP and Google Workspace
Federation	SAML 2.0 federation with Microsoft 365 / Entra ID and Google Workspace; eduGAIN participation via the national federation's metadata
Account recovery	SMS or email verification code; time and attempt limits; reCAPTCHA
Messaging	SMTP accounts; Net GSM, Turatel and Sanal Santral SMS providers; priority order across accounts
Authorisation and audit	Role-based admin rights; IP allow-list; session, action, admin, API, SMS, email and error logs
Interface language	Turkish and English
Delivery	Installed on the organisation's server with nginx, PHP-FPM, PostgreSQL and Beanstalkd; identity provider and admin panel on separate subdomains

DEPLOYMENT Installed on the organisation's server (physical or virtual) with nginx, PHP-FPM and PostgreSQL; the identity provider and admin panel run on separate subdomains. Source import and OpenLDAP/Zimbra account synchronisation run as command-line jobs and a background service.

Book a demo or request a quote

Contact us to see the product in your own environment and discuss scope and pricing.

PHONE +90 850 441 3 441
+90 324 350 03 50
EMAIL bilgi@martateknoloji.com.tr
WEB martateknoloji.com.tr
ADDRESS Mersin Teknopark 35C/B5, Çiftlikköy,
33343 Yenişehir / Mersin, Türkiye
Mersin · İzmir · London

© 2026 Marta Teknoloji A.Ş. — Information in this brochure is for guidance; feature scope may vary by version and deployment.