

## • API-driven Mobile & Web App Security

- Increase login rates by presenting appropriate authentication methods
- Reduce friction with self-service capabilities
- Meet high security demands without custom code
- Deliver a smooth, pixel perfect login experience
- Confidently include standard-compliant security in your DevOps toolchain
- Manage all your users with a single standardized API



## A Secure Foundation for Your Identities and APIs



Allow simple login with existing username and password in a Web form that supports account linking, self-service & Single Sign-on (SSO)



Enable a secure and frictionless login experience across your entire user base. Confirm identities, enable multi-factor authentication even on feature phones or provide an authentication app that displays your brand



Quickly deploy authentication methods out of the box for standard-compliant providers, as well as non-standard & legacy ones, or build your own with our supported SDK



Integrate any mobile, web or single-page application as well as your APIs and microservices in a few lines of code with modern industry-standards like OAuth 2, OpenID Connect, JWT and Assisted Token



Issue tokens using a full-blown scripting language based on JavaScript, enabling even the most advanced token issuance, revocation, exchange and introspection scenarios



Designed for DevOps where every single interaction can be scripted, automated, version controlled and easily used in continuous delivery processes

## All-In-One Features You Need

- ✓ User self-service
- ✓ Social, single- & multi-factor login
- ✓ Unlimited branding possibilities
- ✓ Account linking
- ✓ Complete token issuance language
- ✓ Secure iframe login
- ✓ 100% scriptable administration
- ✓ OpenID Connect Certified

## Supported Integration Standards

- |                  |            |
|------------------|------------|
| ✓ OAuth 2        | ✓ HTML 5   |
| ✓ OpenID Connect | ✓ SCIM     |
| ✓ SAML           | ✓ LDAP     |
| ✓ Kerberos       | ✓ JOSE/JWT |

## Run On-premise or in the Cloud



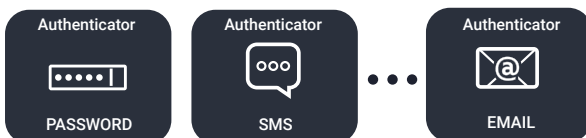
## MODERN AUTHENTICATION

Authentication is more than user login. A modern authentication service enables multi-factor authentication, user self service, account linking and much more. Modern applications require the ability to control and customize the appearance and flows on a per app basis, while maintaining central control and achieving the effect of Single Sign-On.



### Multi-factor Authentication

Curity creates advanced multi-factor possibilities by chaining authentication methods as needed. A common scenario is to combine username/password with a second factor such as an SMS, a keyfob or an app. This reduces the risk of accounts being compromised due to password theft.



### User Self-Service

Curity enables users to manage their own account information. This allows them to create accounts, recover forgotten passwords, change passwords, or be reminded of their username. This greatly reduces the support burden imposed by authentication and registration. All changes are stored in your own user repository, which can be integrated via SCIM, SQL, LDAP or your own API.

### Ready for Web and Mobile SSO

Let the user navigate seamlessly between mobile apps and websites in the mobile browser without having to re-authenticate. Using OpenID Connect, Curity has built in support for single sign-on between mobile apps and between mobile apps and mobile web pages.

### Control User Flows with Actions

Every organization requires different login flows. Using Authentication Actions, the administrator can graphically design the login flow to enforce requirements of the organization. These include looking up additional data about the user, denying access based on user attributes and displaying screens for user action.

### Branding

The templating system built around layering, allowing you to overlay existing templates with your choice of colors, logos and fonts. It is even possible to completely style the look and feel with fully customizable templates. You can mix and match built-in and custom templates as needed. Curity's user-facing screens can be tailor made to suit your needs. Also, the branding can be customized for each client application

### User Account Linking

Modern applications must support a wide range of authentication methods. Social login simplifies signup and access to non-sensitive data, whereas usernames and passwords are familiar and sufficient for some assets. In case of high-worth data, stronger authentication is required. Regardless of the form of credential used, applications need a stable user ID to associate data with. Account linking can be used to accomplish this. Curity makes this otherwise complicated procedure simple and secure. It is available out of the box.



### Essential Features

- ✓ Multi-factor authentication
- ✓ User self registration
- ✓ User password reset
- ✓ Single Sign-On
- ✓ Customizable look and feel
- ✓ Branding per application
- ✓ SDK for custom integrations
- ✓ Configurable input validation

## OAUTH AND OPENID CONNECT SERVER

*The Curity Identity Server is the most advanced OAuth and OpenID Connect server available on the market. A highly configurable server that allows the organization to use and leverage these technologies to their full extent.*



### Scriptable Token Issuance

Curity provides a dynamic scripting language to control token issuance. Very complicated token issuance can be encoded in a simple JavaScript-based language. Tokens can be embedded within other complicated JSON data structures. JavaScript procedures are checked for errors at configuration time, ensuring correctness, and are compiled to deliver the highest possible performance during run-time.

### Expiring Scopes

OAuth scopes represent rights or permissions granted to an app. Sometimes rights should be revoked after a certain period of time while others remain. Implementing such a use case is easy with Curity because each scope can have its own specific expiration time. As tokens are used, the associated permissions and power of tokens are reduced as expired scopes are removed.

### Token Exchange

In token-based systems, an API will often pass on its token to a down-stream API. Not all APIs can be trusted to handle tokens with the same information. In such cases, Curity allows tokens to be exchanged securely between microservices and systems.

### Phantom Tokens

JSON Web Tokens (JWT) are popular to use for their simplicity, but can often compromise privacy. Curity provides the Phantom Token pattern to have highly secure, opaque tokens used by applications on the Internet which are translated into internal JWTs on the internal network.

### Single Page Applications

Using OAuth protected APIs from a Single Page Application (SPA) has been a difficult problem since their inception. Curity provides a simple flow, the Assisted Token Flow, to secure and integrate SPAs with only a few lines of JavaScript and HTML.

- ✓ OpenID Connect Certified
- ✓ OAuth 2.0 Compliant
- ✓ Dynamic client registration
- ✓ OAuth security extensions such as PKCE
- ✓ Pairwise Pseudonym support
- ✓ Device flow for input constrained devices

## USER MANAGEMENT FOR APIS USING SCIM 2.0

*SCIM 2.0 is the most widespread standard for API based user management. Curity lets you attach to any database and deploy a SCIM API on top to unify access.*



### One API To Manage All Users

User CRUD has never been easier. SCIM 2.0 enables customer management applications, support portals and other applications to read and write user data using a standardized REST-based protocol.

### Attach To Any Data Source

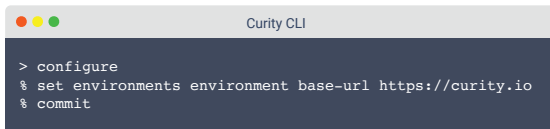
Modernize access to your existing data sources. Curity provides out of the box support for a number of databases, LDAP directories and repositories.

## Configuration and Administration

All configuration in Curity can be managed manually or programmatically, using:

- Command Line Interface (CLI)
- REST API
- Web User Interface

Changes – whether a single setting or numerous alterations – are performed in a single transaction, succeeding or failing as a whole. This ensures that Curity is always running in a consistent state. All configuration can be extracted from a running system, versioned controlled, shared between environments, and rolled back.



```

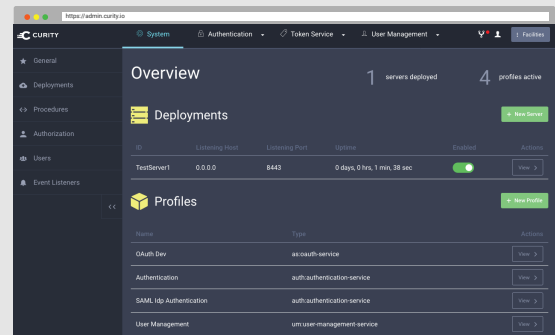
Curity CLI
> configure
% set environments environment base-url https://curity.io
% commit
  
```

## Extensibility

New authentication methods and account storage can be added through supported extension points. Numerous ways are included, and new ones can be created with the SDK. Connect your user repository via LDAP, JDBC or SCIM. Plug in your mail server, SMS provider, and other facilities used by standard components. Reduce the amount of custom code in your login service to the absolute minimum, but ensure that it meets your needs.

## Deployment

Curity runs on-premise or in the cloud. By depending only on Linux & Java, getting started is really fast. Its self-contained distribution allows you to setup an OAuth and OpenID Connect server with advanced features in minutes! The configuration API and the command line interface (CLI) covers 100% of its functionality, making it straightforward to include in your DevOps.



*The Admin User Interface*

## Why Curity?

Curity® was created to solve identity management in an API-driven world. The Curity Identity Server enables organizations to take advantage of best of breed protocols like OAuth, OpenID Connect and SCIM, when providing secure digital services to their users.

The digital identities of organizations are becoming more and more important. The Curity Identity Server is deployed on-premise or in your favourite cloud-provider, making it possible to adopt and operate according to your requirements. The ability to customize is essential: design your specific flows and logic for login; decide on the type of authentication mechanisms to be used when and how; and define the content and format of security tokens.

With Curity, you stay in control on how your digital identities are managed with a ready-made security solution for all your apps, websites, APIs and identities.

## ABOUT CURITY

Curity is the leading supplier of API-driven identity management, providing unified security for digital services. Curity Identity Server is the world's most powerful OAuth and OpenID Connect Server; it is used for logging in and securing millions of users' access to web and mobile apps over APIs and microservices. Curity is built upon open standards and designed for development and operations. We enjoy the trust of large organizations in financial services, telecom, retail, energy and government services with operations across many countries which have chosen Curity for their enterprise-grade API security needs.

To learn more, visit us at <https://curity.io>

Curity® is a registered trademark of Curity AB.

© Curity AB