

OPENOTP SECURITY SUITE

ENTERPRISE-GRADE ALL-IN-ONE
MFA & IAM SOLUTION

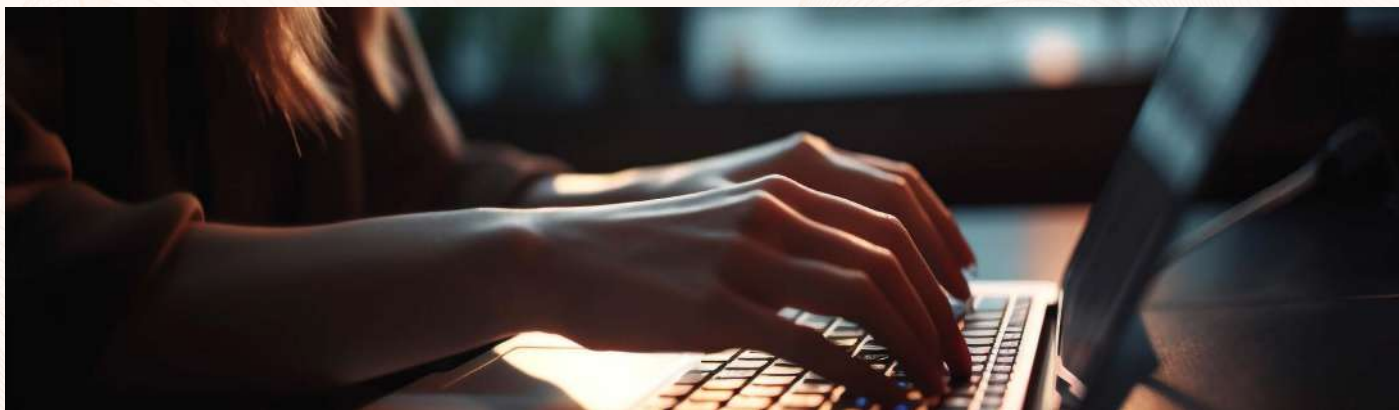


THE MOST COMPLETE MFA SOLUTION TO DATE

OpenOTP Security Suite is far more than a simple multi-factor authentication server. It is the Swiss Army knife of authentication, offering a wide range of 2FA methods and APIs, integrating with any enterprise application or service, whether hosted in the cloud or on-premise

OUR COMPANY

As a European software editor specialized in Identity and Access Management (IAM) and Multi-Factor Authentication (MFA) RCDevs Security provides modular and flexible security solutions, available both on-premise and as a SaaS. Recognized for its software reliability and high customer satisfaction, RCDevs supports small businesses and large businesses alike, across all industries worldwide.



THE POWER OF THE WEBADM PLATFORM

Much more than a simple MFA server, OpenOTP Security Suite is a modular IAM platform powered by **WebADM**, combining centralized identity management with unmatched flexibility.

Centralized & Unified Management

WebADM centralizes both local and **cloud identity management** (Active Directory, OpenLDAP, Entra ID, Google Workspace, etc.) for unified administration, even in hybrid environments.

Advanced Access Control

The **admin interface** allows the creation of fine-grained access policies per system, user, or group, enabling precise and customized security management.

Scalable Solution

OpenOTP Suite combines power, simplicity and agility to provide **access management** that evolves with your business.

FEATURES & BENEFITS

Multiple Identity Sources

→ Ideal for **hybrid environments** combining multiple local directories (LDAP/AD) and **cloud identity services** (Entra ID, Duo, Okta, Ping Identity, etc.).

High Availability

→ **Active-active clustering** ensures continuous service uptime and hassle-free upgrades.

Identity Management

→ **LDAP** and **cloud identities** can be managed through web interfaces or APIs.

Redundancy

→ Automatic failover guarantees uninterrupted access to essential services.

Modular Architecture

→ Scalable architecture that can be easily extended to utilize all system capabilities and features.

HSM Integration

→ Supports **Hardware Security Modules** (HSMs) to encrypt sensitive data such as token keys.

HOW IT WORKS

OpenOTP Security Suite integrates with your existing infrastructure and deploys multi-factor security without complexity.



Native Identity Connectivity

OpenOTP interacts in real time with your identity sources, **local or cloud**, via dedicated connectors ensuring simple, continuous integration.



Centralized Access Policies

Define precise access rules based on users, groups and contextual factors (IP address, time, geolocation, etc.). Authentication dynamically adapts to the assessed risk level.



Flexible Authentication Methods

OTP, mobile push, FIDO2, Passkeys, SMS, e-mail, Smartcard, Magic Links... Choose **methods that best fits your needs**.



Transparent Integration

OpenOTP supports a wide range of integrations through plugins, APIs and standards (RADIUS, LDAP, SAML2, OIDC & OAuth2).



Smooth User Experience

Users authenticate quickly through a simple **second factor**, enhancing security while simplifying adoption.

AUTHENTICATION METHODS



OpenOTP Token App

Mobile Push
or OTP Token



PKI

Certificate-based
authentication



Magic Links

QRCode via eMail or SMS
to confirm access



YubiKey

YubiOTP,
OATH-HOTP & PIV



FIDO2

Public-key cryptography-based
authentication



Software Tokens

Event-based & time-based
OATH tokens



Hardware Tokens

Event-based & time-based
OATH tokens



Legacy Methods

OTP via SMS, eMail & secure
eMail or printed list

APPLICATIONS & THIRD-PARTY SERVICES

Universal RADIUS

Protect **access to your VPNs**
& network devices (Citrix,
Cisco, Pulse Secure, F5, etc.).

LDAP Authentication Security

The LDAP proxy adds MFA
to any application supporting
the LDAP protocol.

ADFS Compatibility

Provides MFA for all ADFS
authentication flows, **including**
Outlook Web Access, Office 365,
SharePoint, and more.

Federated Identity & SSO

Supports **OpenID Connect,**
OAuth 2.0, and SAML2 for secure
federated authentication with
Single Sign-On.

MacOS Sessions

Strengthen macOS logins
with built-in multi-factor
authentication.

Windows Environments

Protect Windows desktops
and RDS sessions with flexible
MFA suitable for complex
infrastructures.

Wi-Fi & Wired Networks

Secure network access via strong
authentication using **EAP-TLS**
and EAP-TTLS protocols.

Unix/Linux Environments

Add MFA to all your Linux/
UNIX services that rely
on **PAM authentication**
mechanisms.

Offline Authentication

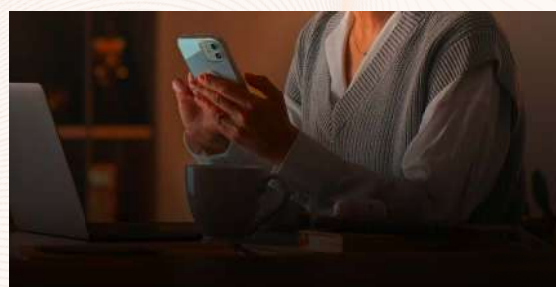
MFA support in **offline mode**
for Windows and macOS using
FIDO2 keys or the OpenOTP
Token app.

APIs

Custom, automatable
integrations optimized
for DevOps environments.

Library

Development libraries
available for C, C++, PHP,
Python, and .NET...



OFFICIAL TOKEN APPLICATION

Our free **OpenOTP Token** application provides Push
notifications in various formats, complementing
traditional OTP methods.

It also includes advanced features such as **OpenOTP**
badging, phishing attempt alerts, geomapping,
biometric protection and electronic signature
capabilities.



DEPLOYMENT MODES

RCDevs adapts to your infrastructure requirements with multiple deployment options, ensuring flexibility, performance and security.

On-Premise

Deploy locally on **physical, virtual or Docker** environments. RCDevs provides Debian/RPM repositories and ready-to-use appliances.

Dedicated Private Cloud

Hosted by RCDevs on dedicated infrastructure or within your own private cloud.

Hosted SaaS

Turnkey solution, hosted and managed by our teams, immediately accessible without installation.



ELECTRONIC SIGNATURE

Multi-level Support

Simple, advanced and qualified electronic signatures compliant with regulatory requirements.

Access-linked Contracts

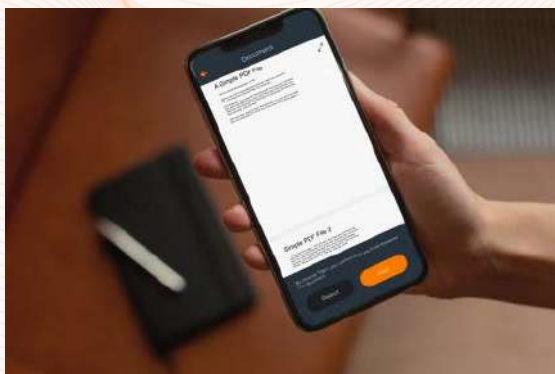
System access is blocked until a document (e.g., NDA) is electronically signed. The signature workflow with the user is fully automated.

Ready-to-use Integrations

Plugins available for **Nextcloud**, **Postfix** (trigger signature via email with attachment), and **Windows** (instant signature via right-click on a document).

Open APIs

Easily integrate electronic signatures into your third-party applications via our APIs.



INCLUDED SELF-SERVICES

Administration Help-Desk

Intuitive web application offering a **simple interface** for first-level IT support and daily operations management with your users.

User Self-Service Desk

Allows users to manage the enrollment of their tokens, **FIDO/Passkeys**, certificates, authentication methods, and badging operations.

Secure Password Reset

Web application accessible at any time or on demand, allowing users to reset their AD, LDAP, Entra ID, etc., passwords.

User Self-Registration

Simplify and automate user enrollment by sending **secure unique links**, offering immediate access to the enrollment portal.



BADGING

Ensure secure access to your enterprise systems with fine-grained management based on user location and authorized zones or countries.

Automatic Password Rotation

User passwords are automatically renewed with each **badging** operation, enhancing security.

Default Locked Account

The user account remains unusable until access is explicitly requested via badging.

Custom Access Policies

Access to a system can be conditioned by prior badging, either from a mobile device or **via the self-service portal**.

Automated Badging

The operation is automatically triggered when the device and network authentication (Wi-Fi or wired) are integrated with RCDevs **NAC system**.