RCDevs
security solutions

ALL-IN-ONE MFA-IAM ENTERPRISE SOLUTION
# OPENOTP™ SECURITY SUITE

THE MOST COMPREHENSIVE MULTI-FACTOR AUTHENTICATION SOLUTION TO DATE

OpenOTP Security Suite is more than your every day Multi-Factor Server. It is a Swiss army knife of authentication, featuring an extensive array of 2FA methods and vast range of APIs, that integrates with any enterprise application or service whether in the cloud or on-premise.

OFFICIAL RECOMMENDED TOKEN APP

Our free **OpenOTP Token App** features Push Notifications and OTPs, badging, e-signature, anti-phishing, geo-mapping & biometric protection.
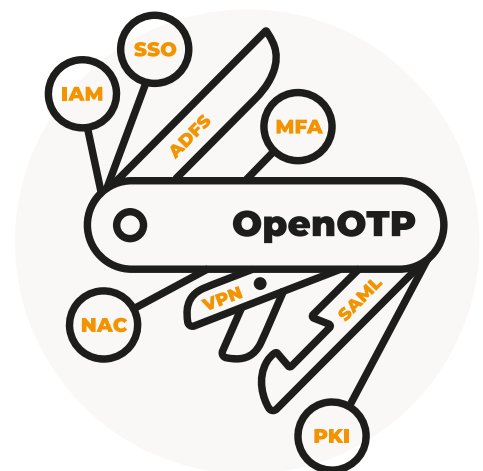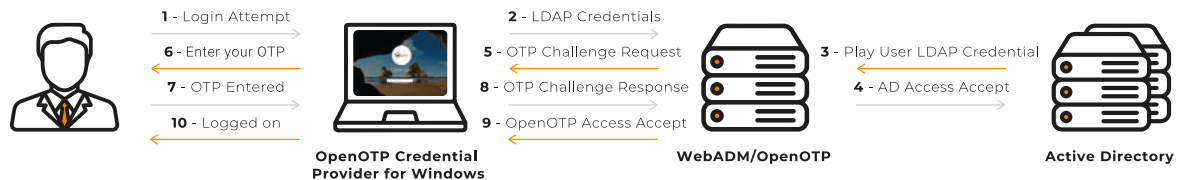

OUR COMPANY

RCDevs is an award winning security company specialized in next-generation multi-factor authentication and PKI. RCDevs is building its growing reputation over high-quality software and complete client satisfaction. RCDevs provides cutting-edge solutions world-wide to clients ranging from SMEs to large scale enterprises in the IT, financial, healthcare, education and government sectors.

POWER OF THE WEBADM PLATFORM

OpenOTP Security Suite is not a standalone Multi-Factor Authentication server, but rather a modular Identity and Access Management platform (WebADM), featuring centralized security audit and pluggable IAM modules which can be individually tuned to address even the most complicated enterprise security requirements. OpenOTP Security Suite provides a seamless AD/LDAP integration, unparalleled to the usual 'read and replicate'. With OpenOTP, you can configure and control 2FA directly from within existing directory accounts. With all data and settings remaining logically in one place, (within the control and perimeter of existing directory) this makes 2FA easier to manage, but also ensures sensitive data is being stored in the most secure and reliable way.

1 - Login Attempt	**2** - LDAP Credentials	**3** - Play User LDAP Credential
6 - Enter your OTP	**5** - OTP Challenge Request	**4** - AD Access Accept
7 - OTP Entered	**8** - OTP Challenge Response	
10 - Logged on	**9** - OpenOTP Access Accept	

OpenOTP Credential Provider for Windows   **WebADM/OpenOTP**   **Active Directory**

Windows login with Two-Factor Authentication

HOW IT WORKS

The heart of the OpenOTP Security Suite is RCDevs' WebADM application platform, in which individual services such as RCDevs Identity Provider (IdP), Multi-Factor Authentication (MFA) and other services run.

To make WebADM features available for your existing directory accounts, simply link the system with a single or multiple ADs, and then add the desired IAM modules.

Thanks to the unique AD/LDAP support in WebADM, rolling out your new 2FA methods is simple: just browse to your AD/LDAP account, group or client policies (VPN, local network...), set the preferred methods of login, issue automated enrollment URLs and test the accounts yourself.

Features / Benefits

Multi-tenancy
➜ Ideal for Managed Service Providers needing to service multiple customer domains with a single WebADM cluster.

Delegated Administration
➜ Ability to delegate user and service control to any third party administrator.

Identity Management
➜ Full Web and API based LDAP identity management capabilities.

HSM
➜ Supports use of HSM to encrypt confidential data such as token keys.

Modular architecture
➜ Highly scalable framework that permits you to easily extend the system's capabilities and add new features.

High-Availability
➜ True active-active clustering for high-availability.

Redundancy
➜ Unparalleled redundancy with the ability to consolidate all services and authentication data to an existing directory implementation, instead of needing to host and manage separate databases.

SUPPORTED AUTHENTICATION METHODS

OpenOTP Token App Mobile Push or OATH Token	**Software Tokens** OATH, Event, Time & Challenge based
PKI User Certificate-based Authentication	**Hardware Tokens** OATH, Event, Time & Challenge based
FIDO2 - Passkeys Public-Key Cryptography Authentication	**Legacy Methods** Printed OATH One-Time Password Mail & Secure Mail - SMS Mobile OTP
Yubikey Tokens Multi-protocol YubiKey Standard & Nano	**Highly Compatible** With OATH Hardware, Software Tokens & OCRA

SUPPORTED LOGIN SCENARIOS

OTP with or without Challenge	OTP concatenated with regular password, provided as separate passcode or separately prompted (i.e. via Challenge-Response).
OTP with or without Domain Password	Domain password can be the first factor, or WebADM can be configured to validate only the OTP. Also ability to set PCI-DSS mode for OTP, in which primary factor failures are not reported back to the logging in user.
OTP with or without PIN	Ability to set an additional PIN factor.
Multi-OTP support	System can allow any user provided OTP, from software or hardware token, Yubikey, SMS and more...
OTP and FIDO2	OTP login combined with use of FIDO2.
Fallback login	System can automatically fallback from one method to another. For example, if user cell phone cannot be reached, an offline OTP method can be initiated.

SUPPORTED THIRD PARTY APPLICATIONS AND SERVICES

Any RADIUS compliant service	Support for MFA login to Citrix, Cisco, Pulse Secure, Checkpoint, Sophos, any RADIUS enabled VPN / SSL-VPN.
Any LDAP compliant service	With RCDevs LDAP Proxy, 2FA can be added on any standard LDAP based authentication.
ADFS enabled services	Support for MFA login to Office365, Outlook Web Application, Sharepoint.
AWS, Salesforce, Google Apps...	Out of the box federation support for several industry standard cloud services.
OpenID Connect and SAML enabled services	Support for any federated web application.
Drupal, Wordpress, Magento, Joomla, Nextcloud	Support plugins available for several industry standard web frameworks.
Wifi Networks	Support for MFA login to Wifi Access Points.
Windows Servers	Support for MFA login to Windows Servers (RDS, RD Gateway).
Unix and Linux servers	Support for MFA login to Unix and Linux machines.
Web APIs	Open and easy to use SOAP and REST APIs for custom web applications.
SDKs	Development libraries for C, C++, PHP, Java, .NET, ASPX.

SUPPORTED USER DIRECTORY MODELS

Standalone internal LDAP — Default Novell eDirectory or OpenLDAP shipping within WebADM. Ideal when needing to create a new segregated directory, i.e. for external accounts.

Direct external LDAP — WebADM connected directly with an existing external LDAP (ActiveDirectory, Oracle Directory, 389, OpenLDAP, etc.). Unparalleled redundancy and control with all authentication and account data in one place, within existing directory objects. No replication or synchronisation of user accounts needed. Optional SQL datastore supported.

Standalone + Direct — WebADM connected with both internal accounts and accounts in an existing external LDAP (both read-only and read-write access options available to external LDAP).

Multi-LDAP (read only) — WebADM connected with multiple external existing LDAPs, in read-only mode (with ability to configure what attributes and objects are read and used in authentication policy decisions). Ideal for Service Providers needing to offer 2FA services to customers managing their own domain.

Multi-LDAP (delegated, high security) — WebADM connected with multiple external existing LDAPs, but in a mode where all authentication and policy data is logically and securely stored directly on the remote directory objects, providing clients with full access and control over their own authentication data. Ideal for Service Providers needing to offer 2FA services to customers with highest available compliance and security mandates.

INCLUDED SELF-SERVICES

Administration Help-Desk
Web application providing an easy-to-use interface for the first level of IT Support function.

Secure Password Reset
Web application and one-time URLs for end users to reset their lost or expired LDAP/AD password.

User Self-Service Desk
Web application to edit your account details, reset password, manage OTP tokens or FIDO devices, etc…

User Self-Registration
Web application to self-register your OTP token or FIDO device after receiving a one-time email or SMS.

MOBILE BADGING

Extra Security
Authorize network access through badging only.

Centralized
Centrally manage and define your workforce's work hours.

Convenient
Badge-in easily with our free OpenOTP Token App.

ELECTRONIC SIGNATURE

On premise
Request Secured Signatures within AD/LDAP users with internal workflows.

API
Extend capabilities of already integrated solutions to suit your enterprise's needs.

Agreement Based Logical Access
Combine legally binding agreements and access to critical systems.

DEPLOYMENT ALTERNATIVES

Private Cloud
Any private cloud. RCDevs also provides a dedicated and fully managed private cloud service.

Virtual Appliance and Software
Our solution is deployed on your own Linux servers (dedicated or virtualized) and operates without any external service dependency.

Docker
Deploy OpenOTP Security Suite in a fully containerized environment.

SaaS
Mutualized or dedicaded cloud.