RCDevs
Security Solutions

ALL FACTORS, ONE SOLUTION
OPENOTP™ MFA SUITE

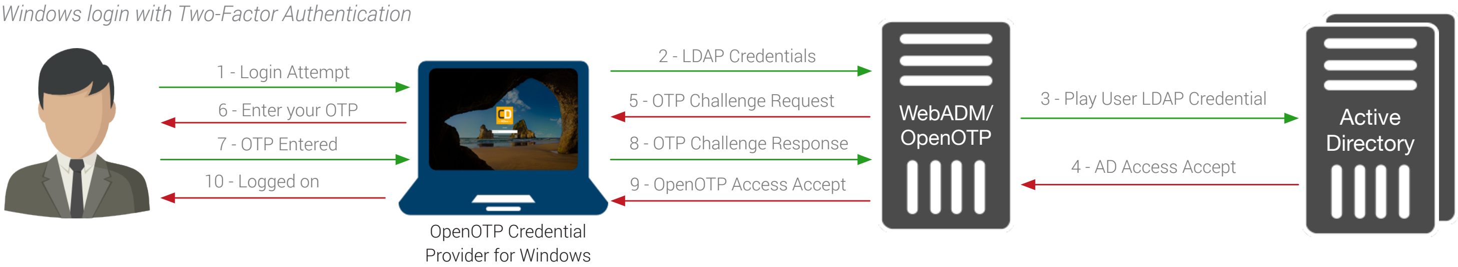
THE MOST COMPREHENSIVE MULTI-FACTOR AUTHENTICATION SOLUTION TO DATE

OpenOTP is more than your every day Multi-Factor Server. It is a multi-factor middleware, 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.

POWER OF PLATEFORM

Unlike other solutions, OpenOTP is not a standalone Multi-Factor Authentication server, but rather a modular Identity and Access Management platform, featuring centralized security audit and pluggable IAM modules which can be individually tuned to address even the most complicated of enterprise security requirements.
OpenOTP provides a seamless LDAP/AD integration, unparalleled to the normal 'read and replicate' approach of competition. With OpenOTP, you can configure and control 2FA directly from within existing directory accounts. All data and settings remain logically in one place, within the control and perimeter of existing directory, making 2FA easier to manage, but also ensuring the sensitive data is being stored in the most secure and reliable way.

Windows login with Two-Factor Authentication


1 - Login Attempt
6 - Enter your OTP
7 - OTP Entered
10 - Logged on
OpenOTP Credential Provider for Windows
2 - LDAP Credentials
5 - OTP Challenge Request
8 - OTP Challenge Response
9 - OpenOTP Access Accept
WebADM/ OpenOTP
3 - Play User LDAP Credential
4 - AD Access Accept
Active Directory

HOW IT WORKS

The heart of the OpenOTP suite is the RCDevs WebADM application platform, on top of 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 LDAP/AD support in WebADM, rolling out your new 2FA methods is then easy: just browse to your LDAP/AD 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.

High-Availability

- True active-active clustering for high-availability.

Powerful Policies

- Fine-grained access control policies per application, network, groups, domains, ...

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.

Modular architecture

- Highly scalable framework that permits to easily extend the system's capabilities and add new features.

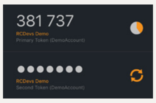
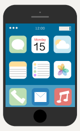
Redundancy

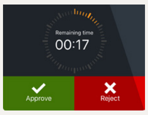
- Unparalleled redundancy with the ability to consolidate all services and authentication data to an existing directory implementation, instead of needing to host and manage separate databases.

HSM

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

SUPPORTED AUTHENTICATION METHODS

Supported Authentication Methods	
	Hardware tokens (RCDevs) 6 and 8 digits OATH TOTP compliant RC200 tokens
	**iOS and Android OTP App** RCDevs OpenOTP software Token
	Google Authenticator, OATH (SW) Any third party OATH TOTP and HOTP compliant software token are supported
	**Out-Of-Band SMS / Email** Pre-fetched and on-demand SMS OTPs OTPs delivered via Email and Secure Email
	Yubikeys Support for Yubikeys
	FIDO U2F Support for Universal 2-Factor devices
	SSH SSH with hardware and software keys

Supported Authentication Methods	
	Hardware tokens (any third party) Any third party OATH TOTP and HOTP compliant hardware tokens are supported
	**iOS and Android Push Notification App** RCDevs OpenOTP Token
	OCRA Full support of OATH-OCRA suites
	QRCode Automated login by scanning a QRCode (requires TiQR)
	Mobile Signature Service ETSI GSM 102 204 MSS API support
	Printed OTP List Printed OATH One-Time Password Lists
	PKI Client certificates with Integrated PKI

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, whether from soft token, hard token, Yubikey or SMS.
OTP and FIDO U2F	OTP login combined with use of FIDO U2F.
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 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.
GoToMeeting, AWS, Salesforce, Google Apps, ...	Out of the box federation support for several industry standard cloud services.
OpenID Connect and SAML enable services	Support for any federated web application.
Drupal, Wordpress, Magento, Joomla, OwnCloud	Support plugins available for several industry standard web frameworks.
Wifi Networks	Support for MFA login to Cisco 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, ...). Unparalleled redundancy and control with all authentication and account data in one place, within existing directory objects. Neither replication nor synchronisation of user accounts needed. Optional SQL datastore supported.

✓ Standalone + Direct

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

✓ Multi-LDAP

WebADM connected with multiple external existing LDAPs, in optional read-only mode (with ability to configure which 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.

✓ SELF-SERVICES INCLUDED

Secure password reset

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

Account self administration

Customizable web portal for end users to edit their personal LDAP/AD account information.

Secure token enrollment

Customizable web portal for end users to enroll tokens and manage their preferred methods of login.

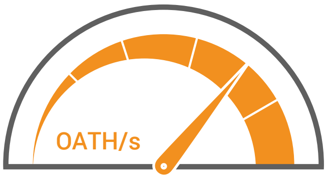
✓ DEPLOYMENT ALTERNATIVES

Private cloud

Virtual infrastructure on Amazon AWS with direct VPN access. RCDevs provides a dedicated and fully managed private cloud service.

Virtual appliance and software

Virtual Appliance (OVF) for ESXi and MS Hyper-V or installer packages for any Linux distribution, solution is deployed on your own servers (dedicated or virtualized) and operates without any external service dependency.



✓ SCALING & PERFORMANCES

Throughput

200 OATH transactions per second on a standalone server.
300 OATH transactions per second on a HA cluster.

User volumes

Single cluster can support environments of over 100.000 users.

✓ LICENSING MODELS

Freeware license

Free license permitting up to 40 users at no cost. All features included, except High-Availability and encryption of configuration data. Only community support available.

Enterprise license

Commercial license starting at 50 users. All features, including High-Availability and encryption of configuration data. Perpetual and Subscription license available with RCDevs Enterprise Support and Maintenance.

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 customer satisfaction. RCDevs provides cutting-edge solutions world-wide to customers ranging from SMEs to large scale enterprises in the IT, financial, healthcare and government sectors.