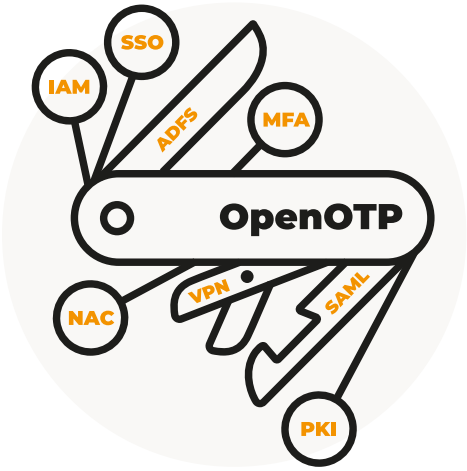
RCDevs
security solutions

SOLUTION D'ENTREPRISE DE MFA-IAM TOUT-EN-UN

OPENOTP™ SECURITY SUITE

LA SOLUTION DE MFA LA PLUS COMPLÈTE À CE JOUR

OpenOTP Security Suite est bien plus que votre serveur d'authentification multi-facteurs quotidien. C'est le couteau suisse de l'authentification, offrant un large éventail de méthodes d'authentification 2FA et une vaste gamme d'APIs, qui s'intègre avec toute application ou service d'entreprise, que ce soit dans le cloud ou on-premise.



APPLICATION TOKEN OFFICIELLE

Notre application gratuite **OpenOTP Token App** offre des notifications Push en plus des OTPs. Mais également du badging mobile, des notifications anti-phishing, du géo-mapping, de la protection biométrique, ainsi que de la signature électronique.

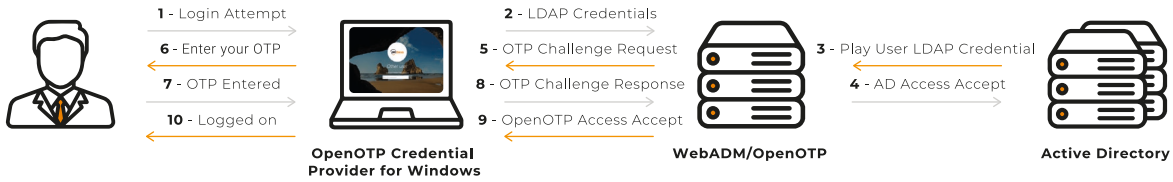
NOTRE ENTREPRISE

RCDevs est une entreprise de sécurité primée spécialisée dans l'authentification multi-facteurs de nouvelle génération et la PKI. RCDevs construit sa réputation croissante sur des logiciels de haute qualité et la satisfaction complète des clients. RCDevs propose des solutions de pointe à des clients du monde entier, allant des PME aux grandes entreprises dans les secteurs informatique, financier, de la santé, de l'éducation et gouvernemental.

LA FORCE DE LA PLATEFORME WEBADM

OpenOTP Security Suite n'est pas seulement un serveur d'authentification multi-facteurs autonome, mais plutôt une solution modulaire (WebADM) d'identité et de gestion des accès (IAM), offrant une auditabilité centralisée et des modules IAM plug-and-play qui peuvent être adaptés individuellement pour répondre aux exigences de sécurité d'entreprise les plus complexes. OpenOTP Security Suite offre une intégration AD/LDAP transparente, inégalée par la méthode habituelle de 'lecture et réplication'.

Avec OpenOTP, vous pouvez configurer et contrôler le 2FA directement à partir de vos comptes d'annuaire existants. Avec toutes les données et paramètres restant en un seul endroit (dans le contrôle et le périmètre de l'annuaire existant), cela rend la 2FA plus facile à gérer, mais assure également que les données sensibles sont stockées de la manière la plus sécurisée et fiable.



Windows login avec 2FA

COMMENT ÇA FONCTIONNE

Le cœur de OpenOTP Security Suite est la plateforme WebADM, dans laquelle des services individuels tels que RCDevs Identity Provider (IdP), l'authentification multi-facteurs (MFA) et d'autres services s'exécutent.

Pour rendre les modules WebADM disponibles pour vos comptes d'annuaire existants, il suffit de lier le système avec un ou plusieurs ADs, puis d'ajouter les modules IAM souhaités.

Grâce au support unique AD/LDAP dans WebADM, déployer vos nouvelles méthodes d'authentification 2FA est simple: il suffit de naviguer vers votre compte AD/LDAP, groupe ou politiques client (VPN, réseau local...), définir les méthodes de connexion préférées, générer des URL d'inscription automatisées et tester les comptes vous-même.

Caractéristiques / Avantages

Multi-domaines
→ Idéal pour les sociétés avec de multiples annuaires et/ou domaines.

Délégation d'administration
→ Capacité de déléguer le contrôle des services utilisateur à tout administrateur d'identité tiers.

Gestion d'identité
→ Capacité de gestion des identités LDAP entièrement basées sur le web et les API

HSM
→ Prend en charge l'utilisation de modules de sécurité matérielle (HSM) pour chiffrer des données confidentielles telles que les clés des tokens.

Architecture modulaire
→ Solution évolutive qui vous permet d'étendre facilement les capacités du système et d'ajouter de nouvelles fonctionnalités.

Haute disponibilité
→ Véritable clustering actif-actif pour une haute disponibilité.

Redondance
→ Redondance qui permet de consolider tous les services et interactions de données dans un seul annuaire existant, éliminant le besoin d'héberger et de gérer des bases de données séparées.

MÉTHODES D'AUTHENTIFICATION

App OpenOTP Token Push mobile ou token OATH	**Tokens logiciels** OATH basé sur l'événement et le temps
PKI Authentification basée sur le certificat utilisateur	**Tokens physiques** OATH basé sur l'événement et le temps
FIDO2 - Passkeys Authentification par cryptographie à clé publique	**Méthodes traditionnelles** Liste imprimée d'OTP OATH - Mail & Secure Mail - OTP par SMS
Tokens Yubikey Standard multi-protocole YubiKey & Nano	**Compatible** Avec les tokens physiques et les softwares OATH & OCRA

SCÉNARIOS DE CONNEXION

OTP avec ou sans challenge	OTP concaténé avec le mot de passe, fourni comme code d'accès séparé ou demandé séparément (par exemple, via Challenge-Response).
OTP avec ou sans mot de passe de domaine	Le mot de passe de domaine peut être le premier facteur ou WebADM peut être configuré pour valider uniquement l'OTP. Possibilité également de définir le mode PCS-DI pour OTP où les échecs du facteur principal ne sont pas rapportés à l'utilisateur qui se connecte.
OTP avec ou sans PIN	Capacité de définir un facteur PIN supplémentaire.
Support multi-OTP	Le système peut autoriser tout OTP fourni par l'utilisateur, qu'il provienne d'un logiciel ou d'un token phyiques, Yubikey, SMS et plus encore.
OTP et FIDO2-Passkeys	Connexion OTP combinée à l'utilisation de FIDO2.
Connexion de secours	Le système peut automatiquement basculer d'une méthode à une autre. Par exemple, si le téléphone de l'utilisateur ne peut pas être atteint, une méthode OTP hors ligne peut être initiée.

APPLICATIONS ET SERVICES TIERS

Tout service compatible RADIUS	Support pour la connexion MFA à Citrix, Cisco, Pulse Secure, Checkpoint, Sophos, n'importe quel VPN/SSL-VPN activé RADIUS.
Tout service compatible LDAP	Avec le proxy LDAP RCDevs, la 2FA peut être ajoutée à toute authentification basée sur LDAP standard.
Services activés ADFS	Support pour la connexion MFA à Office365, Outlook Web Application, Sharepoint.
AWS, Salesforce, Google Apps...	Support pour plusieurs services cloud standards de l'industrie.
OpenID Connect et services activés SAML	Support pour toute application web fédérée.
Nextcloud, Wordpress, Magento, Joomla, Drupal	Plugins de support disponibles pour plusieurs frameworks web standards de l'industrie.
Réseaux WiFi	Support pour la connexion MFA aux points d'accès WiFi.
Serveurs Windows	Support pour la connexion MFA aux serveurs Windows (RDS, RD Gateway).
Serveurs Unix et Linux	Support pour la connexion MFA aux machines Unix et Linux.
Web APIs	SOAP ouvert et REST APIs faciles à utiliser pour des applications web personnalisées.
SDKs	Bibliothèques de développement disponibles pour C, C++, PHP, Java, .NET, ASPX.

MODÈLES D'ANNUAIRES UTILISATEURS

✓ **Standalone internal LDAP**	LDAP interne par défaut livré avec WebADM. Idéal lors de la création d'un nouveau répertoire ségrégué.
✓ **Direct external LDAP**	LDAP externe directement connecté avec un LDAP externe existant (ActiveDirectory, Oracle Directory, 389, OpenLDAP, etc.). Une centralisation du répertoire et un contrôle de toutes les données et accès utilisateurs en un seul endroit, avec une synchronisation et une réplication facultatives des comptes utilisateurs. Base de données SQL optionnelle supportée.
✓ **Standalone + Direct**	WebADM connecté avec lecture et droits internes au LDAP externe existant (accès en lecture seule disponible pour le LDAP externe).
✓ **Multi-LDAP (read only)**	WebADM connecté avec de multiples LDAP externes en mode lecture seule, avec la capacité de configurer quels attributs des objets sont lus et rendus utilisant l'authentification dans les politiques. Idéal pour les Service Providers offrant des services de 2FA à des clients qui gèrent leurs propres domaines.
✓ **Multi-LDAP (délégation, haute sécurité)**	WebADM connecté avec de multiples LDAP externes, mais dans un mode où toute l'authentification et les politiques d'accès sont gérées au niveau central, offrant aux clients un contrôle et un accès total sur leur propre authentification. Idéal pour les Service Providers offrant des services de 2FA, à leurs clients, avec les niveaux de conformité et de sécurité les plus élevés disponibles.

SELF-SERVICES INCLUS

Help-Desk d'administration
Application web fournissant une interface facile à utiliser pour le premier niveau de support informatique.

Réinitialisation de mot de passe
Application web et liens URL à usage unique pour les utilisateurs finaux afin de réinitialiser leur mot de passe LDAP/AD oublié ou expiré.

Self-service desk
Service utilisateur pour visualiser les détails de compte, réinitialiser le mot de passe, gérer les OTP ou les dispositifs FIDO, etc.

Self-inscription
Application web pour enregistrer votre OTP ou dispositif FIDO après réception via email ou SMS unique.

MOBILE BADGING

Sécurité supplémentaire
Autorise l'accès réseau uniquement par authentification mobile.

Gestion centralisée
Gérez et définissez les heures de travail de votre personnel de manière centralisée.

Pratique
Authentifiez-vous facilement avec notre application OpenOTP Token.

SIGNATURE ÉLECTRONIQUE

On-premise
Demandez des signatures sécurisées avec les utilisateurs AD/LDAP avec des workflows internes.

API
Étendez les capacités des solutions déjà intégrées pour répondre aux besoins de votre entreprise.

Accès logique basé sur les accords
Combinez des accords juridiquement contraignants et l'accès à des systèmes critiques.

ALTERNATIVES DE DÉPLOIEMENT

Cloud privé
Dans n'importe quel cloud privé. RCDevs fournit également un service cloud dédié et entièrement managé.

Appliance virtuelle et software
Notre solution est déployée sur vos propres serveurs Linux (dédiés ou virtualisés) et opère sans aucune dépendance de service externe.

Docker
Déployez la suite OpenOTP Security dans un environnement complètement conteneurisé.

SaaS
Mutualisé ou cloud dédié.