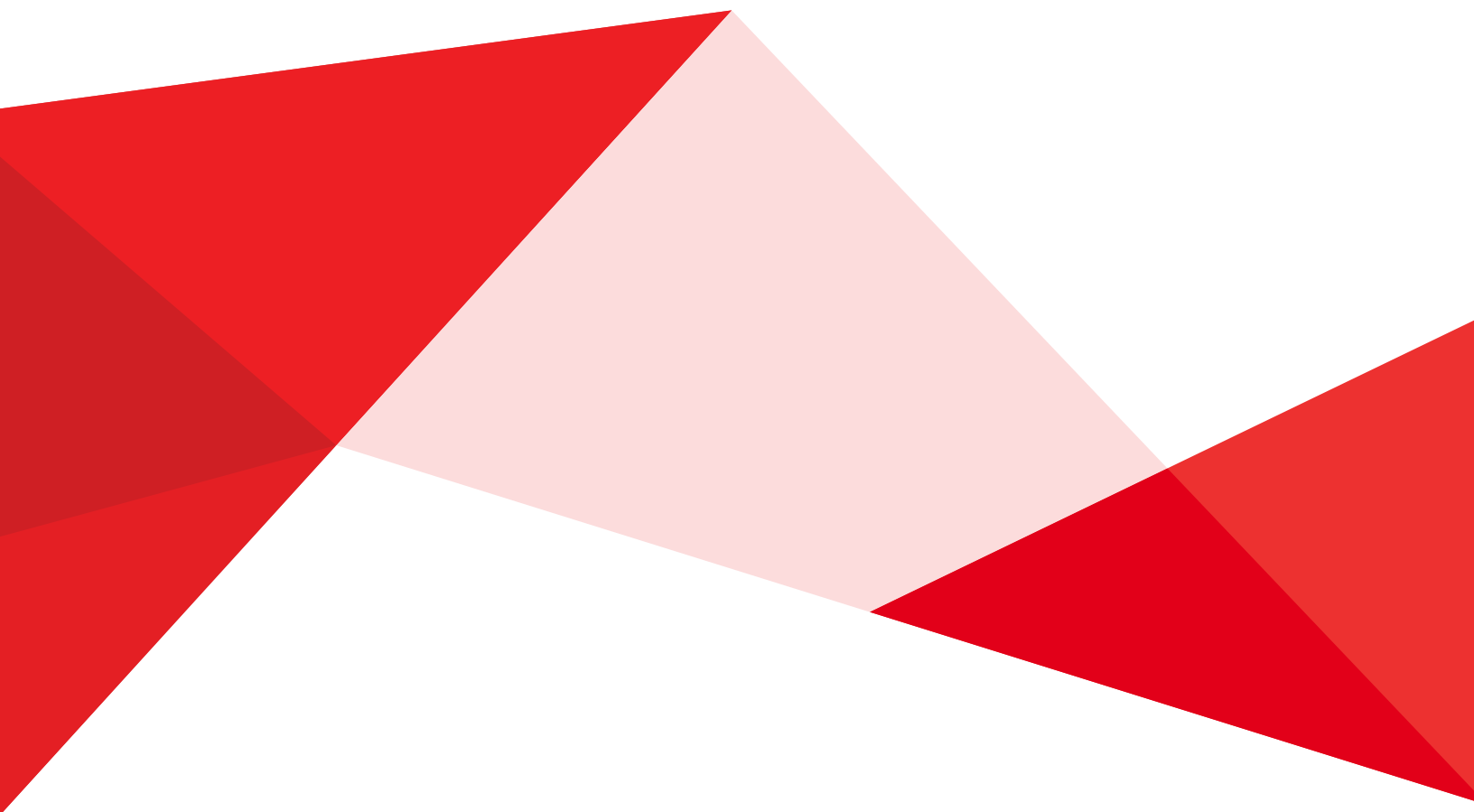




Devolutions
Server

FICHE TECHNIQUE





Devolutions Server

Gestionnaire d'identifiants auto-hébergé conçu pour les professionnels TI

POINTS SAILLANTS

Stockez les informations sensibles dans des coffres sécurisés

Protégez les secrets, identifiants et comptes privilégiés de votre organisation et de vos équipes dans des coffres centralisés. Stockez également des documents sensibles, fichiers, images, et plus encore pour faciliter la consultation en équipe. Liez et injectez les identifiants de manière sécurisée dans les sessions pour rester protégé tout en limitant l'accès en clair.

Gestion flexible des utilisateurs avec l'authentification unique (SSO)

Connectez-vous facilement en vous authentifiant avec [Windows Active Directory](#), [Entra ID \(Azure AD\)](#), [Okta](#) ou [PingOne](#). Utilisez l'authentification locale pour les utilisateurs externes et les invités n'appartenant pas à votre organisation. Des options d'authentification flexibles garantissent la connectivité même lorsque les fournisseurs d'identité sont indisponibles.

Accès sécurisé aux entrées critiques

Créez un système de protection granulaire avec un contrôle d'accès basé sur les rôles (RBAC), permettant de gérer l'accès utilisateur jusqu'au niveau de l'entrée individuelle. Prenez en charge des structures d'autorisations complexes avec un système d'héritage robuste tout en les rendant faciles à maintenir. Utilisez des groupes d'utilisateurs et des ensembles d'autorisations pour attribuer rapidement des droits en masse.

Renforcement de la protection d'accès

Prenez en charge les services MFA via SMS, courriel, Devolutions Workspace, Duo, Yubikey, toute application compatible TOTP et serveur RADIUS. Associez MFA à des politiques d'accès conditionnel pour une protection renforcée avec Entra ID, Okta et PingOne. Appliquez des restrictions basées sur l'adresse IP et la localisation pour empêcher les tentatives de connexion malveillantes et définissez des plages horaires d'accès aux comptes DVLS.

Journalisation et rapports détaillés

Suivez les opérations des utilisateurs et les changements liés aux mots de passe pour établir un historique utile aux audits. Enregistrez tous les événements liés aux entrées et à l'interaction utilisateur, y compris les tentatives de connexion et l'historique, et générez des journaux d'accès complets pour suivre l'activité des utilisateurs privilégiés.

Intégration étroite à l'écosystème Devolutions

Devolutions Server est conçu pour s'intégrer parfaitement avec Remote Desktop Manager, Devolutions Workspace, Devolutions Launcher, Devolutions Send et Devolutions Gateway. Ces outils constituent une boîte à outils complète pour gérer efficacement pratiquement toutes les situations TI.

Solution de gestion des accès privilégiés (PAM) intégrée

Avec le module de gestion des accès privilégiés (PAM), Devolutions Server propose la rotation automatique des mots de passe, l'élévation des privilèges à la demande, et des rapports complets sur les comptes privilégiés. Grâce à des politiques d'emprunt personnalisables et à la prise en charge de fournisseurs de comptes PAM tiers, le module PAM permet de s'adapter à presque tous les fournisseurs d'identifiants et aux besoins de votre équipe.

APERÇU

Les organisations d'aujourd'hui font face à des défis croissants en matière de sécurité et de gestion de l'accès aux ressources TI critiques, de conformité réglementaire et d'efficacité opérationnelle. **Devolutions Server (DVLS)**, source de données auto-hébergée, offre une solution complète qui centralise la gestion des coffres et des connexions à distance, renforce la sécurité et simplifie l'accès pour les équipes de toutes tailles.

DVLS s'intègre parfaitement aux fournisseurs d'identité, applique des contrôles d'accès robustes et offre un système de coffres évolutif pour protéger les données sensibles. Il permet aux équipes TI de mettre en œuvre un contrôle d'accès basé sur les rôles, une rotation automatique des mots de passe via Devolutions PAM, la gestion des sessions à distance et l'élévation des privilèges à la demande, assurant un accès sécurisé et traçable aux ressources sans compromettre la posture de sécurité de l'organisation.

PRINCIPAUX AVANTAGES

Coffre robuste avec contrôles d'accès étendus

- Impose un accès granulaire via le contrôle d'accès basé sur les rôles (RBAC), l'accès conditionnel et les restrictions temporelles ou géographiques.
- Prend en charge plusieurs fournisseurs d'identité et options MFA telles que TOTP, Duo, RADIUS, courriel et SMS.
- Applique des politiques de sécurité cohérentes via les groupes d'utilisateurs et ensembles d'autorisations.
- Permet des demandes d'accès temporaires avec des flux d'approbation pour réduire les privilèges permanents.
- Restreint l'accès selon le type de client, y compris les outils de bureau, navigateur, mobile et CLI.

Intégration approfondie à l'écosystème Devolutions

- S'intègre à Remote Desktop Manager (RDM) pour fournir un accès chiffré aux identifiants avec suivi d'audit complet et prise en charge OTP.
- Améliore Devolutions Launcher grâce à l'utilisation centralisée des identifiants et au contrôle des sessions basé sur les rôles.
- Étend l'accès navigateur avec l'extension Workspace, ajoutant sécurité d'entreprise et journalisation des audits.
- Gère les sessions via Devolutions Gateway avec authentification par jeton, contrôle d'accès, surveillance en temps réel, enregistrement et supervision de session.
- Synchronise les identifiants et permissions sur le web et mobile via Workspace, avec accès hors ligne et flux de demandes.

Journalisation et rapports

- Capture des journaux détaillés pour tous les événements opérationnels, de sécurité et PAM sur l'ensemble de la plateforme.
- Définit des règles personnalisées de conservation et d'archivage pour chaque catégorie de journal avec des durées flexibles.
- Suit des pistes d'audit complètes pour l'utilisation des identifiants, l'activité utilisateur et les modifications de coffre.
- Envoie des alertes par courriel, notifications intégrées, Slack, syslog et messagerie interne sécurisée.
- Génère des rapports couvrant l'administration, la sécurité, l'utilisation PAM et les opérations sur les coffres.

Gestion des accès privilégiés (PAM)

- Sécurise les comptes privilégiés dans des coffres isolés avec accès et visibilité contrôlés.
- Permet l'accès à la demande et l'élévation des privilèges avec flux de demande, approbation, expiration et refus.
- Effectue la rotation automatique des mots de passe selon la politique pour minimiser l'exposition.
- Structure les comptes PAM avec des dossiers et applique des règles via des politiques d'emprunt.
- Journalise toutes les actions privilégiées pour la conformité, l'audit et la visibilité des rapports.

CAS D'UTILISATION

Gestion de mots de passe partagés via Devolutions Server

Une équipe de soutien TI doit accéder en toute sécurité à des identifiants partagés pour les routeurs, serveurs et portails cloud. Plutôt que de transmettre des feuilles Excel ou des notes adhésives, elle utilise Devolutions Server pour stocker et gérer ces identifiants de manière centralisée. Grâce aux contrôles d'accès et à l'audit intégrés, les responsables peuvent s'assurer que seules les bonnes personnes y accèdent et suivre qui a accédé à quoi et quand, assurant ainsi sécurité et conformité.

Combinaison de Remote Desktop Manager avec Devolutions Server

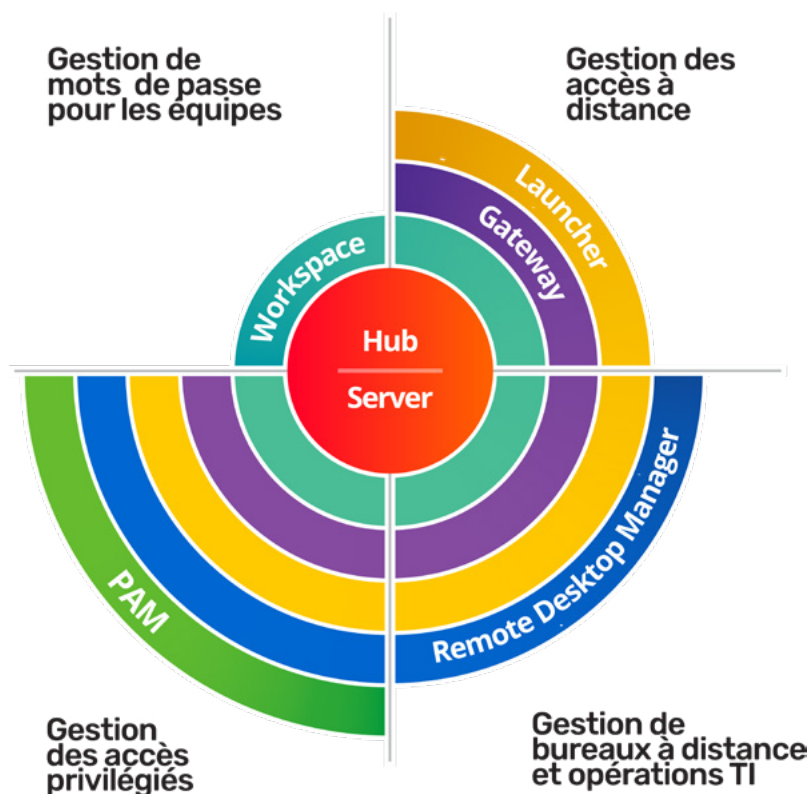
Un administrateur système gère des dizaines de connexions à distance sur plusieurs sites clients. Avec Remote Desktop Manager relié à Devolutions Server, il peut ouvrir n'importe quelle session en un clic, qu'il s'agisse d'une connexion RDP à un serveur Windows ou d'un accès SSH à un serveur Linux. Toutes les données de session, identifiants et historiques de connexion sont stockés de manière sécurisée et centralisée, facilitant l'intégration de nouveaux techniciens sans compromettre la sécurité ou l'efficacité.

Combinaison de Devolutions Gateway avec Devolutions Server

Un consultant travaillant à distance doit dépanner un serveur local d'un client situé derrière un pare-feu, sans configurer un VPN complexe. Avec une instance Devolutions Gateway connectée au Devolutions Server du client, le consultant peut établir une connexion directe et sécurisée au réseau interne pour cette session spécifique — sans tunnel permanent ni redirection de port non sécurisée. C'est rapide, traçable et minimise l'exposition du client aux menaces externes.

Utilisation du module PAM intégré à Devolutions Server

Une organisation ayant des exigences strictes en matière de conformité doit gérer l'accès aux comptes privilégiés comme les administrateurs de domaine ou les identifiants root. Grâce au module PAM intégré à Devolutions Server, l'équipe de sécurité TI peut placer automatiquement ces comptes à haut niveau dans des coffres, planifier la rotation des mots de passe et exiger un processus d'approbation avant l'accès. Lorsqu'un technicien doit exécuter une tâche critique, il demande un accès temporaire, et une fois approuvé, le système enregistre tout, garantissant un contrôle total, la responsabilité et la préparation aux audits.



À PROPOS DE DEVOLUTIONS

Devolutions aide les équipes TI à sécuriser les accès, les identifiants et les connexions à distance via une plateforme intégrée conçue pour la complexité du monde réel.

De la gestion des mots de passe d'entreprise à l'accès privilégié et au contrôle des connexions à distance, nos solutions sont adaptées aux besoins des professionnels TI, des utilisateurs métier et des partenaires externes. Basée au Québec, au Canada, Devolutions reste fièrement indépendante et déterminée à rendre les solutions TI avancées accessibles, conviviales et abordables pour les organisations de toutes tailles.



[Découvrez
nos solutions](#)



[Réservez
une démo](#)



[Des questions
sur les prix ?](#)