LAZAR SOFT

Expert Partner
ManageEngine

FICHE SOLUTION · GESTION DES ACCÈS ET DES IDENTITÉS (IAM)

ManageEngine
Key Manager Plus

Plus aucun certificat n'expire sans prévenir.

Key Manager Plus découvre, consolide, crée, déploie, renouvelle et audite le cycle de vie complet de vos certificats SSL/TLS et de vos clés SSH depuis une console web unique — et rend à vos administrateurs la maîtrise de leurs identités machine.

Certificats SSL/TLS · Clés SSH · Clés PGP · Coffre de clés numériques · Active Directory · Magasin de certificats Microsoft · AWS ACM et IAM

LICENCE À LA CLÉ GÉRÉE · DEUX MODES DE DÉPLOIEMENT

Sur site · Cloud

Tarif éditeur **à partir de 475 €/an** pour 25 clés gérées — grille complète en page 6.

4	Sur site · Cloud	API REST	30 j
FAMILLES D'IDENTITÉS MACHINE GÉRÉES	DEUX MODES DE DÉPLOIEMENT	AUTOMATISATION ET INTÉGRATIONS	ESSAI GRATUIT, SANS CARTE BANCAIRE

LAZAR SOFT
Distributeur & intégrateur ManageEngine en France

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com

Des identités numériques trop nombreuses pour être tenues à la main.

Ce qu'est Key Manager Plus

Key Manager Plus est une solution de gestion des clés et des certificats accessible via une interface web, qui aide les entreprises à découvrir, consolider, créer, déployer, auditer et suivre le cycle de vie des clés SSH et des certificats SSL/TLS.

Les clés SSH et les certificats SSL sont au cœur d'une architecture de sécurité multicouche : ces identités numériques constituent le fondement de la confiance, sur lequel reposent toutes les autres stratégies de sécurité. Elles sont aussi, pour cette raison même, devenues une cible privilégiée. Une fois entré dans l'environnement SSH et SSL d'une organisation, un attaquant étend son accès, vole des identités à privilèges supérieurs et établit des portes dérobées permanentes.

Le problème qu'elle résout

- Les clés SSH ne sont, en général, ni surveillées ni gérées : l'organisation s'expose sans le savoir.
- Sans système automatisé, inventorier les clés, restreindre les privilèges d'accès et assurer leur rotation périodique reste une tâche herculéenne.
- Un environnement SSL/TLS devient vite complexe dès lors que les certificats proviennent de plusieurs autorités de certification, avec des durées de validité variables.
- Un certificat non géré expire sans prévenir : interruption de service, message d'erreur navigateur qui abime l'image de marque, et dans les cas extrêmes violation de sécurité.
- Des certificats non conformes ou invalides peuvent être mis en service sans que personne ne le détecte.

CE QUE LA SOLUTION GÈRE

Certificats SSL/TLS · Clés SSH · Clés PGP · Coffre de clés numériques

MODES DE DÉPLOIEMENT

Sur site — ON-PREMISES

Cloud — SAAS

PRÉREQUIS SERVEUR

Processeur Dual Core minimum · **RAM** 8 à 16 Go · **Disque** 11 à 31 Go
Windows 11, 10, Server 2016 et supérieur · **Linux** Ubuntu, CentOS, RHEL
Détail complet en page 5.

Le périmètre couvert par la plateforme — du certificat public à la clé PGP

DÉCOUVRIR ET CONSOLIDER

- Découverte des certificats SSL/TLS
- Découverte des clés SSH
- Intégration Active Directory
- Magasin de certificats Microsoft

ACQUÉRIR ET DÉPLOYER

- Génération de CSR
- Workflow de demande de certificat
- Déploiement centralisé
- Création et déploiement des clés
- Rotation périodique des clés

SÉCURISER ET SURVEILLER

- Analyse des vulnérabilités SSL
- Signalement des certificats SHA-1
- Alertes d'expiration
- Renouvellement automatique
- Connexions SSH à distance

AUDITER ET RESTAURER

- Audit et rapports
- Cartographie clés-utilisateurs
- Reprise après sinistre

Le détail de chaque domaine figure aux pages 3 et 4.

Découvrir, acquérir, déployer, renouveler.

Découverte et consolidation

CERTIFICATS SSL/TLS

- **Découvrez l'ensemble du parc** — tous les certificats SSL/TLS déployés sur le réseau sont détectés et versés dans un inventaire centralisé et sécurisé.
- **Quelle que soit leur origine** — la consolidation ne dépend ni du fournisseur, ni de l'algorithme de chiffrement, ni de la durée de validité.
- **Couvrez toutes les sources** — certificats utilisateurs Active Directory, magasin de certificats Microsoft, certificats émis par une autorité de certification Microsoft, serveurs SMTP, équilibreurs de charge, AWS ACM et IAM, certificats auto-signés.
- **Gérez les certificats d'Active Directory** — découvrez, importez et gérez les certificats associés aux comptes utilisateurs, et automatisez leur gestion via l'intégration avec votre autorité de certification Microsoft.
- **Relancez les analyses périodiquement** — les scans automatisés maintiennent l'inventaire à jour sans intervention.

Demande, acquisition et déploiement

WORKFLOW DE CERTIFICAT

- **Générez vos CSR instantanément** — l'outil de génération de requêtes de signature est intégré à la console.
- **Demandez et obtenez vos certificats** — processus de demande simplifié auprès des autorités de certification tierces de confiance, avec validation automatisée du contrôle de domaine.
- **Automatisez avec Let's Encrypt** — l'intégration couvre l'acquisition, le déploiement, le suivi et le renouvellement.
- **Exploitez votre AC privée** — la solution embarque des capacités d'autorité de certification interne, en complément des AC publiques.
- **Déployez de façon centralisée** — les certificats nouvellement acquis ou renouvelés sont poussés vers les serveurs finaux correspondants.

Analyse des vulnérabilités SSL

CERTIFICATS SSL/TLS · SERVEURS FINAUX

- **Analysez après déploiement** — certificats et serveurs finaux sont contrôlés une fois la mise en service effectuée.
- **Détectez les vulnérabilités connues** — Heartbleed, POODLE, suites de chiffrement faibles et état de révocation des certificats (CRL, OCSP).
- **Corrigez les configurations fragiles** — identifiez les paramétrages SSL vulnérables et les chiffrements faibles, et remplacez les certificats révoqués.
- **Signalez les certificats SHA-1** — repérez et remplacez ceux qui reposent encore sur cette fonction de hachage obsolète.

Expiration et automatisation du cycle de vie

CERTIFICATS SSL/TLS

- **Évitez les interruptions de service** — les alertes périodiques et personnalisables protègent contre l'expiration silencieuse d'un certificat en production.
- **Allez au-delà de la simple alerte** — le renouvellement et la gestion du cycle de vie s'automatisent, sans intervention manuelle.
- **Orchestrez d'un seul geste** — configurés une fois, les workflows enchaînent acquisition, déploiement, actions post-déploiement et renouvellement.
- **Encadrez les accès** — des restrictions par rôle déterminent qui peut agir sur quel certificat.
- **Reliez la solution à votre chaîne d'outils** — intégrations contextuelles avec les solutions ITSM et MDM, et API REST pour l'automatisation.

Inventorier, faire tourner, auditer.

Découverte et consolidation des clés SSH

CLÉS SSH

- **Détectez toutes les clés du réseau** — les ressources SSH sont découvertes automatiquement et versées dans un référentiel centralisé et sécurisé.
- **Associez les utilisateurs à leurs clés** — chaque ressource découverte est rattachée aux utilisateurs et à leurs clés privées respectives.
- **Consolidez l'existant** — toutes les clés découvertes rejoignent le référentiel de Key Manager Plus.
- **Prenez en charge quatre types de clés** — RSA, DSA, ECDSA et ED25519.

Création, déploiement et rotation

CLÉS SSH

- **Créez de nouvelles paires de clés** — la génération s'opère de manière centralisée depuis la console.
- **Associez et déployez en masse** — les clés sont rattachées aux utilisateurs puis poussées sur les systèmes cibles.
- **Programmez la rotation** — des tâches planifiées font tourner automatiquement les clés SSH à intervalles réguliers, ce qui prévient les abus de privilèges.
- **Repartez d'une base saine** — supprimez les relations de confiance existantes entre utilisateurs et clés publiques, ou créez et ajoutez de nouvelles clés.
- **Appliquez une politique de création** — des règles strictes encadrent la production des clés.

Accès distant et cartographie

CLÉS SSH · UTILISATEURS

- **Ouvrez une session SSH en un clic** — les connexions vers les systèmes distants se lancent depuis la console, de manière centralisée.
- **Cartographiez les relations clés-utilisateurs** — une représentation graphique restitue, à l'échelle de l'organisation, quelle clé est associée à quel compte.
- **Importez vos utilisateurs** — depuis Active Directory, un annuaire LDAP ou un serveur RADIUS, individuellement ou par groupes.
- **Attribuez des rôles** — chaque utilisateur reçoit un rôle d'accès et une politique de mot de passe.

Clés PGP et coffre de clés

CLÉS PGP · CLÉS NUMÉRIQUES

- **Créez et gérez vos clés PGP** — attribuez les opérations autorisées à la paire de clés, posez des alertes d'expiration et suivez les opérations réalisées.
- **Disposez d'un coffre dédié** — tout autre type de clé numérique peut y être stocké, récupéré, mis à jour et géré depuis la même interface.
- **Auditez de la même façon** — ces identités bénéficient des mêmes rapports détaillés que les clés SSH et les certificats.

Audit, rapports et reprise après sinistre

TOUTES LES IDENTITÉS GÉRÉES

- **Établissez un mécanisme d'audit inviolable** — les enregistrements couvrent l'ensemble des activités des utilisateurs et des dispositions prises.
- **Générez des rapports complets** — sur les diverses opérations de gestion des clés et des certificats, accessibles instantanément.
- **Pilotez depuis un tableau de bord unique** — vue d'ensemble immédiate de toutes les opérations SSL et SSH.
- **Planifiez vos sauvegardes** — l'intégralité de la base de données est sauvegardée à intervalles réguliers pour assurer la reprise après sinistre.

Ce qu'il faut prévoir avant l'installation.

ORGANISATION	CLÉS GÉRÉES	PROCESSEUR	RAM	DISQUE
Petite	moins de 500	Dual Core / Core 2 Duo	8 Go	800 Mo + 10 Go
Moyenne	500 à 1 000	Quad Core	8 Go	800 Mo + 20 Go
Grande	plus de 1 000	Octa Core	16 Go	1 Go + 30 Go

Capacités minimales ; un socle supérieur est évidemment accepté. Disque : espace produit + espace base de données. Le terme « clés » désigne le total des clés privées SSH, des certificats SSL/TLS et de toute autre clé numérique gérée — c'est aussi l'unité de licence : la même grandeur détermine le dimensionnement du serveur et le tarif.

Socle logiciel

WINDOWS

- Windows 11 · Windows 10
- Windows Server 2025 · 2022 · 2019 · 2016

LINUX

- Ubuntu 18.x et supérieur
- CentOS 6.x et supérieur
- Red Hat Enterprise Linux 5.x et supérieur
- Fonctionne également en machine virtuelle

BASE DE DONNÉES ET COMPOSANTS

- PostgreSQL 15.7, embarqué avec le produit
- MS SQL Server 2016 et supérieur, en base externe (installé sur Windows Server 2016 ou supérieur)
- Apache Tomcat et runtime Java embarqués

NAVIGATEURS

- Microsoft Edge, sous Windows
- Chrome, Firefox, Ulaa, Safari et Brave, sous Windows, Linux et macOS

À prévoir en amont

INSTALLATION

- Aucune installation logicielle préalable : le matériel et le socle logiciel ci-dessus suffisent.
- Un serveur SMTP externe reste indispensable au fonctionnement du serveur et à l'envoi des notifications.

AUTHENTIFICATION ET ACCÈS

- Compte local, Active Directory, LDAP ou RADIUS
- Rôles d'accès et politiques de mot de passe
- API REST et API SSH pour l'automatisation

POUR LA DÉCOUVERTE SSH ET SSL

- Un compte de service disposant de droits administrateur local ou équivalents sur le serveur Key Manager Plus et sur les systèmes cibles.
- Microsoft .NET Framework 4.5 ou supérieur.

PORTS À OUVRIR

- 6565 console web (HTTPS) · 53306 PostgreSQL
- 22 SSH · 443 HTTPS · 389 LDAP · 636 LDAPS
- 135 WMI/MSCA · 445 SMB

Spécifications techniques

AUTORITÉS DE CERTIFICATION INTÉGRÉES

- Let's Encrypt · Microsoft CA · GoDaddy · Sectigo · Symantec · Thawte · GeoTrust · RapidSSL · DigiCert
- Autorité de certification privée intégrée

DÉCOUVERTE SSL PRISE EN CHARGE

- Certificats utilisateurs Active Directory
- Magasin de certificats Microsoft et certificats émis par une AC Microsoft
- Serveurs SMTP · Équilibreurs de charge
- AWS ACM et IAM · Certificats auto-signés

ALGORITHMES ET LONGUEURS DE CLÉ

- Clés privées SSL — RSA, DSA, EC
- Clés SSH — RSA, DSA, ECDSA, ED25519
- Longueurs 1 024, 2 048, 4 096 bits
- Signature SHA-256, SHA-384, SHA-512
- Keystores JKS et PKCS12

DÉTECTION DE VULNÉRABILITÉS SSL

- Heartbleed · POODLE
- Suites de chiffrement faibles
- État de révocation — CRL, OCSP

04 — LICENCE ET TARIFS

Une seule variable : le nombre de clés gérées.

Abonnement annuel, tarif éditeur, de 25 à 25 000 clés gérées.

CLÉS GÉRÉES	SUR SITE	CLOUD
25	475 €	599 €
50	745 €	899 €
100	1 075 €	1 299 €
200	1 345 €	1 599 €
300	1 545 €	1 849 €
500	2 045 €	2 449 €
1 000	2 645 €	3 199 €

CLÉS GÉRÉES	SUR SITE	CLOUD
2 000	3 945 €	4 749 €
3 000	5 045 €	6 049 €
5 000	7 195 €	8 649 €
10 000	13 795 €	16 549 €
15 000	16 795 €	20 149 €
20 000	19 795 €	23 749 €
25 000	22 795 €	27 349 €

Licence perpétuelle — sur site

de 1 188 € à 56 988 €

Achat unique. Maintenance et support annuels en sus, à 20 % de la licence.

Cloud — facturation mensuelle

de 59 € à 2 735 €/ mois

Alternative à l'abonnement annuel cloud ci-dessus.

Évaluation

30 jours

Édition complète, sans carte bancaire.

L'accompagnement LAZAR SOFT

Sur devis

Comptage réel avant chiffrage, preuve de concept, installation, formation, support en français.

Tarifs publics éditeur — source : ManageEngine, page de tarification Key Manager Plus, consultée le 13/08/2026. Montants repris à parité avec les tarifs publiés en dollars par l'éditeur (1 $ = 1 €), sans conversion de change. **L'éditeur applique par ailleurs une marge de change hors zone américaine** : ces montants sont un ordre de grandeur, pas un prix de vente. Prix indicatifs et non contractuels ; les paliers intermédiaires font l'objet d'un chiffrage sur mesure. Devis personnalisé LAZAR SOFT sur demande.

Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com