

# Notes de version de GroupWise Messenger

Octobre 2023

- ♦ « Nouveautés » page 1
- ♦ « Configuration système requise » page 2
- ♦ « Instructions d'installation » page 2
- ♦ « Problèmes connus » page 3
- ♦ « Compatibilité avec les autres systèmes de messagerie instantanée (sous Linux et Mac) » page 4
- ♦ « Documentation Messenger » page 5
- ♦ « Mentions légales » page 5

## Nouveautés

Reportez-vous aux sections ci-dessous pour obtenir des informations sur les nouveautés spécifiques à chaque version.

- ♦ « GroupWise Messenger 23.4 » page 1
- ♦ « GroupWise Messenger 18.5 » page 1
- ♦ « Nouveautés des versions antérieures de Messenger » page 2

## GroupWise Messenger 23.4

Les corrections de sécurité apportées dans cette version sont les suivantes :

- ♦ Mise à jour d'OpenSSL vers la version 3.0.9
- ♦ Mise à jour de la bibliothèque libcurl vers la version 8.1.2

## GroupWise Messenger 18.5

Les améliorations apportées dans cette version sont les suivantes :

**Base de données mise à jour :** GroupWise Messenger 18.5 dispose d'une base de données mise à jour et des instructions de migration sont incluses dans l'image de la version. Si vous mettez Messenger à niveau vers la version 18.5, reportez-vous à la section [GroupWise Messenger 18.5 et versions ultérieures : détails de la migration de la base de données](#) avant d'effectuer l'opération. La migration est obligatoire si vous effectuez une mise à niveau vers la version 18.5 à partir de Messenger 18.1.x ou d'une version antérieure.

**Mise à jour de la chaîne de chiffrement par défaut :** afin de continuer à respecter les normes de sécurité les plus strictes, GroupWise et Messenger 18.5 incluent une chaîne de chiffrement par défaut mise à jour. Si vous devez modifier la chaîne par défaut en fonction de la version actuelle que vous utilisez, vous pouvez la remplacer à l'aide du paramètre de chaîne de chiffrement `sslCipherSuite` dans les fichiers de démarrage de l'agent après la mise à niveau vers la version 18.5. Pour plus d'informations, reportez-vous aux sections pertinentes relatives au paramètre de démarrage des agents dans le [GroupWise Administration Guide](#) (Guide d'administration de GroupWise).

## Nouveautés des versions antérieures de Messenger

Pour consulter le contenu de la section « Nouveautés » des versions de Messenger antérieures à la version 18.5, reportez-vous aux [Notes de version de GroupWise Messenger 18](#).

## Configuration système requise

La configuration système requise pour GroupWise Messenger 18 et versions ultérieures (y compris la configuration requise pour les périphériques mobiles) est répertoriée à la section « [GroupWise Messenger Hardware and Software Requirements](#) » (Configuration matérielle et logicielle requise pour GroupWise Messenger) du manuel *GroupWise Messenger Installation Guide* (Guide d'installation de GroupWise Messenger).

## Instructions d'installation

Les instructions d'installation complètes sont disponibles dans le [GroupWise Messenger Installation Guide](#) (Guide d'installation de GroupWise Messenger).

## GroupWise Messenger 18.5 et versions ultérieures : détails de la migration de la base de données

GroupWise Messenger stocke des données comprenant des paramètres, des configurations, des listes de contacts utilisateur, des stratégies et d'autres informations dans deux bases de données ArangoDB sur la machine du système Messenger. Les anciennes versions d'ArangoDB prenaient en charge deux types de formats de base de données : `mmfiles` (memory-mapped files) et `rocksdb`.

La version originale d'ArangoDB utilisée par GroupWise Messenger 18.0.x et 18.1.x était ArangoDB 3.3 et, par défaut, le format de base de données sous-jacent choisi pour les nouvelles instances était `mmfiles`. Avec ArangoDB 3.4, le format par défaut pour les nouvelles instances est passé à `rocksdb`, et avec ArangoDB 3.7, il n'est plus possible d'utiliser `mmfiles` comme format de base de données.

GroupWise Messenger 18.2.x - 18.4.x utilise ArangoDB 3.4, qui prend en charge les deux formats, mais la valeur par défaut est `rocksdb` pour les nouvelles instances.

GroupWise Messenger 18.5 utilise ArangoDB 3.10, qui ne prend en charge que le format `rocksdb`. Nous avons effectué cette modification pour des raisons de sécurité ; les anciennes versions d'ArangoDB présentent des problèmes de sécurité critiques de haut niveau.

Si vous avez initialement créé votre ou vos systèmes Messenger à l'aide d'une version antérieure à GroupWise Messenger 18.2.0, vos bases de données utilisent le format `mmfiles`. GroupWise Messenger 18.5 et les versions ultérieures ne fonctionneront pas avec ces anciennes bases de données. Le script `install.sh` dans

l'image 18.5 détecte ce cas et interrompt l'installation si les bases de données sont dans l'ancien format. Nous avons ajouté le fichier `migrate.txt` à l'image avec des instructions pour la migration des bases de données de l'ancien format vers le nouveau format, `rocksdb`, afin que GroupWise Messenger puisse être installé.

Si les bases de données sont très volumineuses (la taille de la base de données d'archivage peut devenir assez importante), la procédure de migration peut prendre beaucoup de temps et utiliser une grande quantité d'espace disque. Pour cette raison, nous avons décidé de ne pas effectuer de migration automatisée pour le moment.

## Problèmes connus

Les problèmes connus suivants ont été identifiés. Les versions concernées par ces problèmes sont indiquées et des solutions sont proposées le cas échéant.

- ♦ [« Problème potentiel avec les clés de chiffrement OpenSSL après la mise à niveau vers GroupWise Messenger 18.5 » page 3](#)
- ♦ [« Les erreurs d'installation d'AVX et de SSE4.2 empêchent la mise à niveau vers Messenger 18.5 » page 4](#)
- ♦ [« Problèmes connus des versions antérieures de Messenger » page 4](#)

## Problème potentiel avec les clés de chiffrement OpenSSL après la mise à niveau vers GroupWise Messenger 18.5

Les agents GroupWise Messenger utilisent désormais la version 3.0.8 d'OpenSSL, qui est une mise à niveau d'OpenSSL 1.1.1 qui était la version utilisée dans GroupWise 18.4.2 et ses versions antérieures. Cette nouvelle version d'OpenSSL ne prend pas en charge les clés chiffrées qui utilisaient l'algorithme DES-CBC (`des`) ; les clés chiffrées de cette manière doivent de nouveau être chiffrées au moyen d'un algorithme ultérieur, tel que DES-EDE3-CBC (`des3`).

Les clés plus anciennes chiffrées au format PKCS#5 afficheront le texte suivant en haut du fichier :

```
-----BEGIN RSA PRIVATE KEY-----  
Proc-Type: 4, ENCRYPTED  
DEK-Info: DES-CBC, 6555BB78F9C56E96
```

Notez l'ancien algorithme DES-CBC non pris en charge dans la ligne DEK-Info pour PKCS#5. Malheureusement, les clés chiffrées au format PKCS#8 affichent uniquement la ligne suivante, sans indiquer si le problème existe :

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

Les agents GroupWise Messenger 18.5 et GroupWise 18.5 ne s'exécuteront pas et afficheront des erreurs de configuration SSL si leurs clés ont été chiffrées au moyen de l'ancien algorithme. L'administration de GroupWise, WebAccessNG et MARS ne sont pas concernés par ce problème.

**Résolution** : la procédure suivante permet de convertir une clé chiffrée avec l'algorithme `des` vers l'algorithme `des3`. Pour ce faire, vous avez besoin d'accéder à l'*utilitaire de ligne de commande openssl*. Avant de commencer, vous devez repérer l'existence d'un problème et identifier la ou les clés à rechiffrer à l'aide des informations fournies ci-dessus. Le chemin d'accès au dossier de certificats dans lequel les fichiers de clé sont conservés sur le serveur Messenger est indiqué ci-dessous :

```
/opt/novell/messenger/certs
```

Substitutions des noms de fichiers pour les chaînes de commande :

- ♦ `withpassword.key` : nom utilisé pour désigner le fichier de la clé devant être rechiffrée.

- ♦ `nopassword.key` : nom utilisé pour désigner le fichier de la clé qui représente le fichier temporaire.
- ♦ `withdes3pw.key` : nom utilisé pour désigner le fichier de la clé qui représente le fichier de clé correctement chiffré.

Procédure :

- 1 Exécutez cette commande pour convertir le fichier de la clé chiffré par mot de passe en fichier de clé sans mot de passe :

```
openssl rsa -in withpassword.key -out nopassword.key
```

---

**REMARQUE** : si le fichier de clé d'origine a été créé sans mot de passe et qu'il est disponible, vous pouvez ignorer cette étape et commencer à l'étape 2.

---

- 2 Exécutez cette commande sur la clé sans mot de passe pour ajouter un mot de passe à l'aide de l'algorithme `des3` :

```
openssl rsa -in nopassword.key -des3 -out withdes3pw.key
```

- 3 Sauvegardez le fichier de clé initial, puis remplacez-le par le nouveau fichier de clé généré, en utilisant le même nom que le fichier initial.
- 4 Relancez les agents.

## Les erreurs d'installation d'AVX et de SSE4.2 empêchent la mise à niveau vers Messenger 18.5

GroupWise Messenger 18.5 dispose d'une base de données mise à jour qui nécessite la prise en charge du processeur pour les jeux d'instructions SSE4.2 et AVX. Si votre système Messenger s'exécute sur des périphériques avec des UC qui ne prennent pas en charge SSE4.2 ou AVX, vous devez continuer à exécuter Messenger sur une version antérieure (par exemple, 18.4.x) jusqu'à ce que vous ayez mis à niveau votre matériel.

Pour vérifier si les UC de votre serveur Messenger prennent en charge SSE4.2 et AVX, exécutez les commandes suivantes :

- ♦ `cat /proc/cpuinfo | grep sse4_2 > /dev/null 2>&1`
- ♦ `cat /proc/cpuinfo | grep avx > /dev/null 2>&1`

Si une commande ne renvoie rien, le jeu d'instructions n'est pas pris en charge.

## Problèmes connus des versions antérieures de Messenger

Pour consulter la section « Problèmes connus » des versions de GroupWise Messenger antérieures à la version 18.5, reportez-vous aux [Notes de version de GroupWise Messenger 18](#).

## Compatibilité avec les autres systèmes de messagerie instantanée (sous Linux et Mac)

---

**IMPORTANT** : les systèmes Messenger tiers mentionnés dans cette section ne prennent pas en charge les connexions clients simultanées disponibles avec Messenger 18.

---

L'application de messagerie instantanée Adium pour Max OS X est disponible sur le [site Web d'Adium \(https://adium.im/\)](https://adium.im/).

Le connecteur de messagerie instantanée Open Source Pidgin (anciennement Gaim) est disponible sur le [site Web de Pidgin \(http://www.pidgin.im\)](http://www.pidgin.im).

Le plug-in de messagerie instantanée Open Source Kopete est disponible sur le [site Web de Kopete \(http://kopete.kde.org/index.php\)](http://kopete.kde.org/index.php).

## Documentation Messenger

Les sources suivantes fournissent des informations concernant GroupWise Messenger :

- ♦ Documentation en ligne sur le produit : [site Web de documentation de GroupWise](#).
- ♦ Documentation produit incluse dans GroupWise Messenger: cliquez sur le menu **Aide** dans le coin supérieur droit du client Messenger.

## Mentions légales

Copyright 1993-2023 Open Text.

Les seules garanties pour les produits et services d'Open Text et ses sociétés affiliées et fournisseurs de licence (« Open Text ») sont telles qu'elles sont énoncées dans les clauses de garantie expresse qui accompagnent ces produits et services. Rien dans le présent document ne doit être interprété comme constituant une garantie supplémentaire. Open Text ne sera en aucun cas tenu responsable des erreurs ou omissions techniques ou de rédaction contenues dans le présent document. Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.