

GroupWise Messenger Release Notes

October 2023

- ♦ “What’s New” on page 1
- ♦ “System Requirements” on page 2
- ♦ “Installation Instructions” on page 2
- ♦ “Known Issues” on page 3
- ♦ “Compatibility with Other Instant Messaging Systems (on Linux and Mac)” on page 4
- ♦ “Messenger Documentation” on page 4
- ♦ “Legal Notices” on page 5

What’s New

Reference the sections below for What’s New information specific to each version.

- ♦ [“GroupWise Messenger 23.4”](#) on page 1
- ♦ [“GroupWise Messenger 18.5”](#) on page 1
- ♦ [“What’s New for Earlier Messenger Versions”](#) on page 2

GroupWise Messenger 23.4

The following security fixes were made in this release:

- ♦ Updated OpenSSL to 3.0.9
- ♦ Updated the libcurl library to 8.1.2

GroupWise Messenger 18.5

The following enhancements were made in this release:

Updated database: GroupWise Messenger 18.5 has an updated database and migration instructions are included in the release image. If you are upgrading Messenger to 18.5, reference the [GroupWise Messenger 18.5 and Later - Database Migration Details](#) before you upgrade. Migration is mandatory if you are upgrading to 18.5 from Messenger 18.1.x or earlier versions.

Updated default cipher string: In keeping with maintaining the highest security standards, GroupWise and Messenger 18.5 include an updated default cipher string. If you need to modify the default string based on the current version that you have, you can override it using the cipher string switch `sslCipherSuite` in the agent startup files after upgrading to 18.5. For information, see applicable “startup switch” sections for the agents in the [GroupWise Administration Guide](#).

What’s New for Earlier Messenger Versions

To see the “What’s New” content for Messenger versions that pre-date 18.5. See the [GroupWise Messenger 18 Release Notes](#).

System Requirements

GroupWise Messenger 18 and later system requirements (including requirements for mobile devices) are listed in “[GroupWise Messenger Hardware and Software Requirements](#)” in the *GroupWise Messenger Installation Guide*.

Installation Instructions

Complete installation instructions are available in the [GroupWise Messenger Installation Guide](#).

GroupWise Messenger 18.5 and Later - Database Migration Details

GroupWise Messenger stores data that includes settings, configurations, user-contact lists, policies, and other information in two ArangoDB databases on the Messenger system machine. Older versions of ArangoDB supported two types of database formats: `mmfiles` (memory-mapped files) and `rocksdb`.

The original version of ArangoDB used by GroupWise Messenger 18.0.x and 18.1.x was ArangoDB 3.3, and by default the underlying database format chosen for new instances was `mmfiles`. With ArangoDB 3.4, the default format for new instances changed to `rocksdb`, and with ArangoDB 3.7 it is no longer possible to use `mmfiles` as the database format.

GroupWise Messenger 18.2.x - 18.4.x uses ArangoDB 3.4, which supports both formats, but defaults to `rocksdb` for new instances.

GroupWise Messenger 18.5 uses ArangoDB 3.10, which only supports the `rocksdb` format. We have made this change for security reasons; the older versions of ArangoDB have some critical and high-level security issues.

If you originally created your Messenger system(s) using a version older than GroupWise Messenger 18.2.0, your databases are using the `mmfiles` format. GroupWise Messenger 18.5 and later versions will not run against these old databases. The `install.sh` script in the 18.5 image will detect this case and will terminate the installation if the databases are in the older format. We have added the file `migrate.txt` to the image with instructions for migrating old format databases to the new, `rocksdb` format so that GroupWise Messenger can be installed.

If the databases are very large (the Archive database can get quite large), the migration procedure could take a long time and use up a large amount of disk space. For this reason, we decided not to do an automated migration at this time.

Known Issues

The following known issues have been identified. Where applicable workarounds and versions found in are also provided.

- ◆ [“Potential issue with OpenSSL encryption keys after upgrading to GroupWise Messenger 18.5” on page 3](#)
- ◆ [“AVX and SSE4.2 installation errors prevent upgrade to Messenger 18.5” on page 4](#)
- ◆ [“Known Issues from Earlier Messenger Versions” on page 4](#)

Potential issue with OpenSSL encryption keys after upgrading to GroupWise Messenger 18.5

GroupWise Messenger agents now use OpenSSL version 3.0.8, which is an upgrade from OpenSSL 1.1.1 that was used in 18.4.2 and earlier versions of GroupWise. This new version of OpenSSL does not support encrypted keys that used the DES-CBC algorithm (`des`); keys encrypted this way need to be re-encrypted using a later algorithm, such as DES-EDE3-CBC (`des3`).

Older keys encrypted in the PKCS#5 format will have the following at the top of the file:

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

Notice the old, unsupported algorithm DES-CBC in the DEK-Info line for PKCS#5.

Unfortunately, keys encrypted in the PKCS#8 format will only show the following line, which does not show if the problem exists:

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

GroupWise Messenger 18.5 agents and GroupWise 18.5 agents will not run and will give SSL misconfiguration errors if their keys were encrypted using the old algorithm. GroupWise Administration, WebAccessNG, and MARS are not affected by this issue.

Resolution: The following procedure can be used to convert a key encrypted with `des` to `des3`. This requires access to the *openssl command-line utility*. Before you begin, you need to identify if you have a problem and which key(s) needs to be re-encrypted by using the information provided above. The path to the certificate folder where the key files are maintained on the Messenger Server is shown below:

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

File name substitutions for command strings:

- ◆ `withpassword.key` - Substitute key file name that needs to be re-encrypted.
- ◆ `nopassword.key` - Substitute key file name that represents the temporary file.
- ◆ `withdes3pw.key` - Substitute key file name that represents the correctly encrypted key file.

Procedure:

- 1 Run this command to convert the password-encrypted key file to a key file without a password:

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

NOTE: If the original key file was created without a password and that is available, you can skip this step and start with Step 2.

- 2 With the no password key, run this command to add a password using `des3`:

```
openssl rsa -in nopassword.key -des3 -out withdes3pw.key
```
- 3 Backup the original key file and then replace it with the newly generated key file, using the same name as the original.
- 4 Relaunch the agents.

AVX and SSE4.2 installation errors prevent upgrade to Messenger 18.5

GroupWise Messenger 18.5 has an updated database that requires processor support for SSE4.2 and AVX instruction sets. If your Messenger system runs on devices with CPUs that do not support SSE4.2 or AVX, you should keep Messenger running on an earlier version (for example, v18.4.x) until you have upgraded your hardware.

To see if your Messenger server CPU(s), supports SSE4.2 and AVX, run the following commands:

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

If a command returns nothing, the instruction set is not supported.

Known Issues from Earlier Messenger Versions

To see the “Known Issues” for GroupWise Messenger versions that pre-date Messenger 18.5, reference the [GroupWise Messenger 18 Release Notes](#).

Compatibility with Other Instant Messaging Systems (on Linux and Mac)

IMPORTANT: The third-party messenger systems discussed in this section do not support the simultaneous client connections available with Messenger 18.

The Adium instant messaging application for Mac OS X is available at the [Adium website \(https://adium.im/\)](https://adium.im/).

The Pidgin (formerly Gaim) open source instant messaging connector is available at the [Pidgin website \(http://www.pidgin.im\)](http://www.pidgin.im).

The Kopete open source instant messaging plug-in is available at the [Kopete website \(http://kopete.kde.org/index.php\)](http://kopete.kde.org/index.php).

Messenger Documentation

The following sources provide information about GroupWise Messenger:

- ♦ Online product documentation: [GroupWise Documentation website](#).
- ♦ Product documentation included within GroupWise Messenger: click the **Help** menu in the upper-right corner of the Messenger client.

Legal Notices

Copyright 1993 - 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

