Gallagher Command Centre

Security Health Check Utility 2.06.079

Release Note

Copyright © Gallagher Group Limited

Contents

1 Introduction 3
- 1.1 Purpose 3
- 1.2 New in v2.06.079 3
- 1.3 Compatibility 3

2 Running the utility 4
- 2.1 Running the utility manually on the server 4
- 2.2 Running the utility manually on a workstation 7
- 2.3 Running the utility on a schedule (server only) 9
- 2.4 Running the utility via command line 10

3 Generating your user-friendly SHC Report 11
- 3.1 About the SHC Report 11
- 3.2 Generating the SHC Report 11

4 Known issues 12

Appendix A: Security Health Check Process Map 13

Copyright © Gallagher Group Limited

1 Introduction

This release note is for the Security Health Check Utility v2.06.079 of Gallagher Command Centre.

1.1 Purpose

The Gallagher Security Health Check (SHC) Utility allows you to audit the state of your hardware, operating system, configuration and user-based security. The utility enables you to gain a deeper understanding of your security vulnerabilities and makes recommendations to rectify them. SHC gives you confidence in the configuration of Command Centre, and therefore reduces the need to perform manual checks.

When you run the utility, it performs a number of tests against your Command Centre system and outputs the test results. Based on the utility's findings, each test is given a severity rating of critical, high, medium, low, or no issues. Additionally, each test displays detailed information on potential risks and recommendations on how to rectify the security risks.

Note: Not all issues the utility flags are guaranteed to be problematic as it will depend on the circumstances and other measures in place on a site.

IMPORTANT: Ensure you always run the latest version of the Security Health Check Utility. Otherwise, you may miss vulnerability notifications added in the latest version.

To check the latest version, go to https://products.security.gallagher.com/security/global/en/products/software/integrations/security-health-check/p/INT128

1.2 New in v2.06.079

Enhancements:

- Supports Command Centre up to vEL9.40
- Checks for recently published vulnerabilities that are known in your version of Command Centre.

1.3 Compatibility

This feature introduces the following Gallagher software:

- Gallagher Security Health Check vSHC2.06.079

This utility supports the 10 most recent versions of Gallagher Command Centre. The Security Health Check Utility v2.06.079 supports the following Gallagher software:

- Gallagher Command Centre vEL8.30 - vEL9.40

The utility has been tested using the following Windows operating systems:

- Windows 10 (64-bit)
- Windows 11 (64-bit)
- Windows Server 2019
- Windows Server 2022

Copyright © Gallagher Group Limited

2 Running the utility

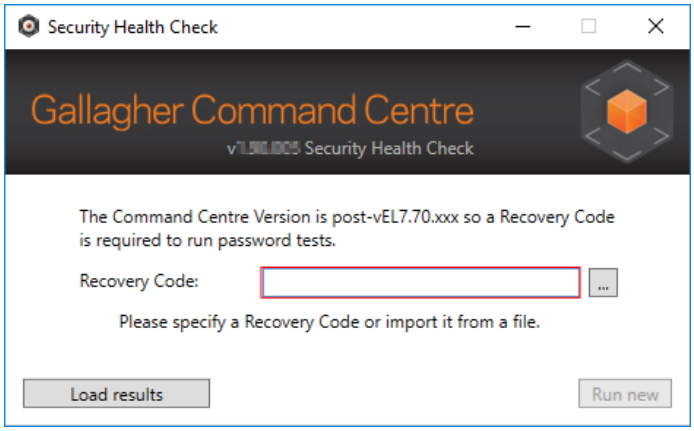
2.1 Running the utility manually on the server

To run the SHC, perform the following procedures on the Command Centre server:

1. Ensure you have the latest version of the Security Health Check Utility. Check the latest version here: https://products.security.gallagher.com/security/global/en/products/software/integrations/security-health-check/p/INT128
2. Double-click the **SecurityHealthCheck.exe**

   The User Account Control window displays.
3. Click **Yes** to continue.

   The SHC Disclaimer window opens.
4. Read the disclaimer, then click **I Agree** to continue.
5. The Security Health Check window opens.



Note: The recovery code is required when you are running this utility on vEL7.70 or later. The recovery code is a 25-character code generated during the installation of the Command Centre Server. The recovery code protects data such as encryption keys and user codes. Generally, the recovery code is used for disaster recovery.

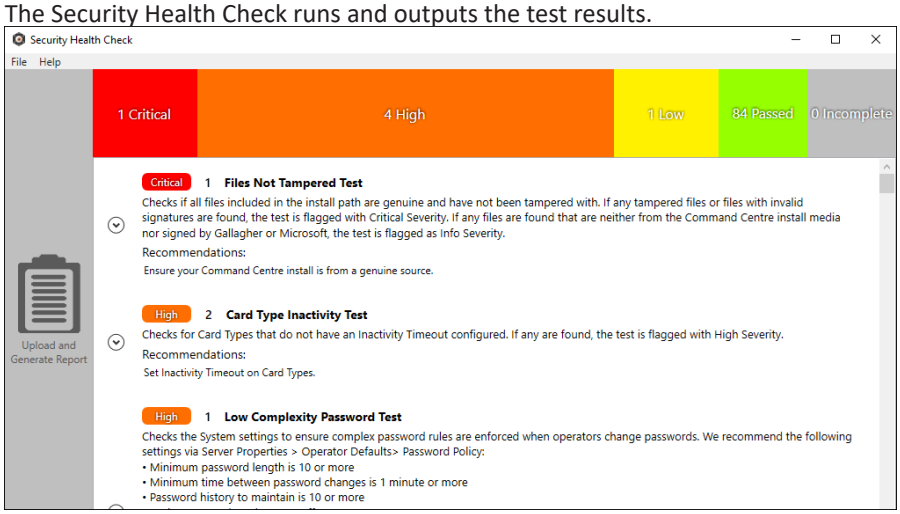
6. Do you want to run a new test or load existing results?

To...	then...
run a new test,	a. If the **Recovery Code** field is already filled with your recovery code, click the **Run new** button. b. If not already filled, click the ... button to select your recovery code. File Explorer opens. c. Locate and double-click on the Command Centre recovery file that was created when Command Centre was installed. d. Click the **Run new** button.

Copyright © Gallagher Group Limited

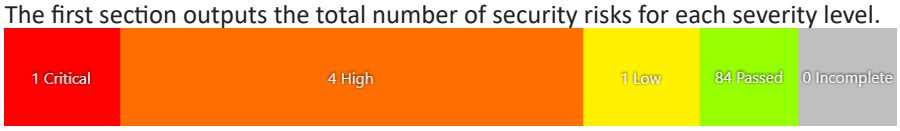
To...	then...
upload past results,	a. Click the **Load results** button. File Explorer opens. b. Navigate to the file location, then select the JSON file. c. Click **Open**.

The Security Health Check runs and outputs the test results.



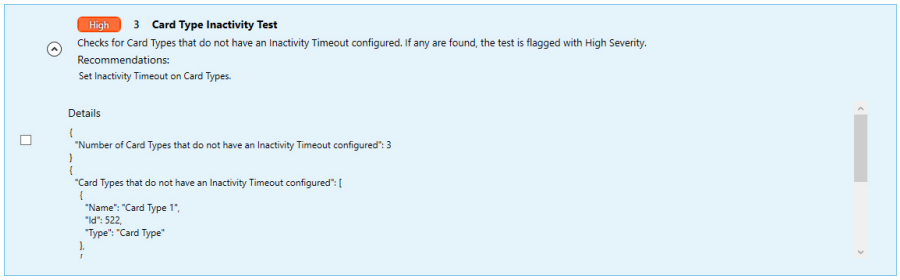
Severity level

The first section outputs the total number of security risks for each severity level.



Tests

In the second section, the utility outputs all the tests and sorts them by severity level. Each row (test) shown has a severity level, the total number of instances for that particular test, the test name, and a description. You can click the ⌄ button to see more details about a test.



Re-run selected test(s)

Once the utility outputs the tests, you can re-run a selected test after you have mitigated an issue identified by the SHC utility.

To re-run the test, select its check box and click the **Retest Selected** button.

Note: Save options are not available after running the selected test(s). Retest all tests to enable save options.

Copyright © Gallagher Group Limited

Saving test results

The full test results contain sensitive information about the site, therefore we recommend that this file is stored securely. It should not be shared with a third party.

The summarised test results do not include sensitive or site-specific information. However, we still recommend that you keep this file in a secure location. And, as stated in the Data Storage Terms section later in this release note, data uploaded for reporting purposes will be stored securely in an encrypted database.

What do you want to do?

To...	then...
Save summarised results	1. On the Command Centre server, click **File** > **Save**. 2. Navigate to the folder you want to save the results to, and click **Save**.

Save full results	1. From the Command Centre server's Start menu, open Command Prompt as administrator.
	2. In the command line, type the location of the folder containing your **SecurityHealthCheck.exe** file, then hit Enter. For example:
	`cd C:\Users\Me\Desktop`
	3. Paste the following into the command line, then hit Enter:
	`start /wait SecurityHealthCheck.exe -f`
	For example:
	`C:\Users\Me\Desktop>start /wait SecurityHealthCheck.exe -f`
	4. Read the warning message. To continue, type the Y key then hit Enter.
	The results are saved to the location as indicated.

Loading existing results

After you run the utility, you can also load existing results.

To load existing results:

1. Click **File** > **Load**.
2. Navigate to the appropriate JSON file and double-click on it.

Copyright © Gallagher Group Limited

2.2 Running the utility manually on a workstation

About running on a workstation: When run on a workstation, the SHC only performs the 'Files Not Tampered' test, which checks if all files included in the install path are genuine and have not been tampered with. There is no option to save or upload the workstation test result. You can load a saved test result that was generated on the Command Centre server.

To run the SHC, perform the following procedures on a Command Centre workstation:

1. On the Command Centre server, navigate to the following folder and copy the file **InstalledThirdPartyFiles.json**:

   `C:\Program Files\Gallagher\Command Centre`

2. Paste this file on the Command Centre workstation in the same folder that the **SecurityHealthCheck.exe** is located in.
3. Ensure you have the latest version of the Security Health Check Utility. Check the latest version here: https://products.security.gallagher.com/security/global/en/products/software/integrations/security-health-check/p/INT128
4. On the workstation, double-click the **SecurityHealthCheck.exe**
5. If the User Account Control window displays, click **Yes** to continue.

   The SHC Disclaimer window opens.
6. Read the disclaimer, then click **I Agree** to continue.
7. The Security Health Check window opens.



8. Do you want to run a new test or load existing results (i.e. results saved from the server)?

To...	then...
run a new test,	click the **Test Client Install** button.
upload past results,	a. Click the **Load results** button. File Explorer opens. b. Navigate to the file location, then select the JSON file. c. Click **Open**. d. Go to Step 11 of this procedure.

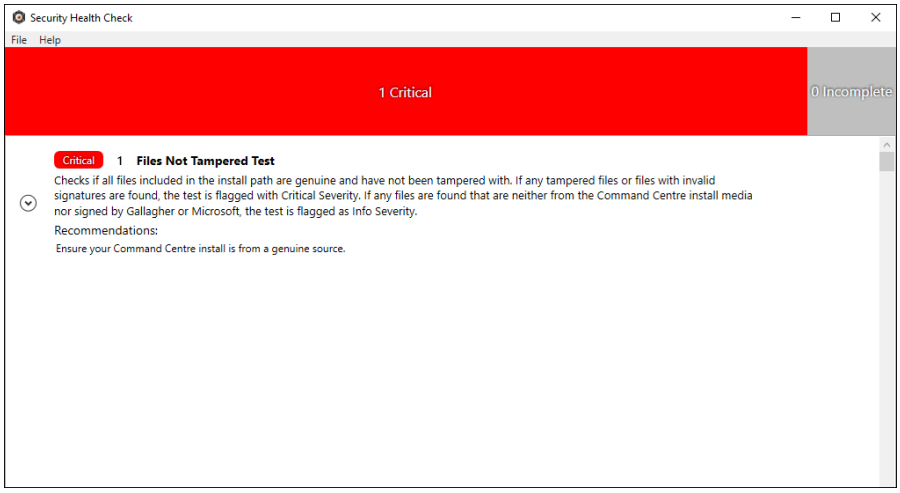
Copyright © Gallagher Group Limited

9. Click the ⌄ button next to **Detected Installations** to see the clients that the utility has detected for testing. If any are missing, manually select them with the ... button(s).

   Note: Only the ClickOnce clients installed for the currently logged-in Windows user are detected. Regular setup workstations are detected for all users. Therefore, if ClickOnce clients have been installed for multiple Windows users on the same workstation, either run the Security Health Check while logged in as each user (once per user), or run the utility (as any user) once for each user, manually selecting the installations for each user each time with the ... buttons (e.g. `C:\Users\[user1]\...`).

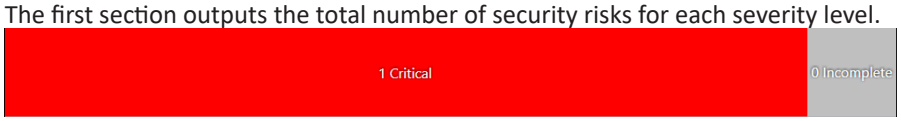
10. Click the **Run new** button to run the 'Files Not Tampered Test' on the detected clients.

11. The Security Health Check runs and outputs the test results.



Severity level

The first section outputs the total number of security risks for each severity level.



Tests

In the second section, the utility outputs the 'Files Not Tampered Test' result. The test result has a severity level, the total number of instances for that particular test, the test name, and a description. You can click the ⌄ button to see more details about the test.

Re-run selected test(s)

Once the utility outputs the test, you can re-run the test after you have mitigated an issue identified by the SHC utility.

To re-run the test, select its check box and click the **Retest Selected** button.

Loading existing results

You can also load existing results that have been generated and saved from the Command Centre server.

To load existing results:

1. Click **File** > **Load**.
2. Navigate to the appropriate JSON file and double-click on it.

Copyright © Gallagher Group Limited

2.3 Running the utility on a schedule (server only)

Note: This procedure is only possible on SHC v1.30 and later versions, and must be done on the Command Centre server.

To have the SHC utility run and save summarised results automatically on a set schedule, perform the following procedure on the Command Centre server:

Before you begin, ensure you have the latest version of the Security Health Check Utility. Check the latest version here: https://products.security.gallagher.com/security/global/en/products/software/integrations/security-health-check/p/INT128

1. Ensure you have run the SHC utility v1.30 or later version as administrator at least once. Refer to step 2.1 *"Running the utility manually"* earlier in this release note. You needn't save the results, you are only running it to generate an encrypted recovery code.
2. From the start menu, search for and open **Task Scheduler**.

   The Windows Task Scheduler window displays.
3. From the menu bar, select **Action** > **Create Task...**

   The Create Task window displays.
4. Click the **Change User or Group...** button.

   The Select User or Group window displays.
5. In the **Enter the object name to select** field, enter the name of the Windows User to run this scheduled task. This should be the same administrator account as the one that ran the utility in step 1 of this procedure.
6. Click the **Triggers** tab.
7. Click the **New...** button.

   The New Trigger window displays.
8. Set the desired schedule for when the SHC utility will run, then click **OK**.
9. Click the **Actions** tab.
10. Click the **New...** button.

    The New Action window displays.
11. Click the **Browse...** button.
12. Navigate to and select the executable **SecurityHealthCheck.exe**
13. Do you want to save the summarised results in the Security Health Check folder or select another one?

To save summarised results to...	then...
The SHC folder (*Documents*\ *Gallagher Security Health Check*)	In the **Add arguments (optional)** field, enter '-s'.
A different location	In the **Add arguments (optional)** field, enter '-s -o *[your chosen full location path]*'. For example: '-s -o C:\Users\Admin\Desktop'.

14. If required, configure any other Task settings.
15. Click **OK** to save and close the Create Task window.

Result: The SHC utility will run as per your configured schedule.

Copyright © Gallagher Group Limited

2.4 Running the utility via command line

The Security Health Check utility allows some additional arguments when run via command line.

1. On the Command Centre server, use File Explorer to open the folder containing the utility, then hold down **Shift** and right-click an empty space.
2. Select 'Open command window here' or 'Open PowerShell window here'.
3. Type or paste **SecurityHealthCheck.exe -help** (command window) or **.\SecurityHealthCheck.exe -help** (PowerShell) and press enter to view the available arguments.
4. Run the command again with the desired argument.

For more help running the utility via command line, contact the Gallagher Support Team.

Copyright © Gallagher Group Limited

3 Generating your user-friendly SHC Report

3.1 About the SHC Report
3.2 Generating the SHC Report

3.1 About the SHC Report

Using the summarised results of your Command Centre installation, the Security Health Check utility will prepare a user-friendly report. This must be done with the full results generated on the Command Centre server, whether you are running the utility on the server or have loaded the server results onto the utility on a workstation.

The report will include:

- your overall score and protection level
- individual score for all categories: hardware, users, configuration and server settings
- recommendations on how to improve your total score, and
- report findings (tests, severity levels, the total number of instances and recommendations) and changes to your score since your last report (if applicable).

3.2 Generating the SHC Report

Before you begin
To generate the Security Health Check report, the following needs to be allowed for connection on the machine running the Security Health Check utility:

- Port 443 (inbound and outbound)
- healthcheck.security.gallagher.cloud

Perform the following procedure to generate a Security Health Check report:

1. Complete the previous section 2 *"Running the utility"* to either run the utility on the Command Centre server or load existing server results from a JSON file.

   Your test results are displayed in the utility.
2. Within the Security Health Check utility, click the **Upload and Generate Report** button on the left-hand side of the window.

   An information pop-up box displays.
3. If you would like to review what information will be uploaded to generate the report, click the **Review** button to review your summarised results.
4. Click the **Upload** button.
5. Navigate to the folder you want to save the SHC Report to, and click **Save**.

   The Security Health Check utility displays a spinning cogs icon. Once the cogs disappear, your SHC Report will be available in the file location you selected.

Copyright © Gallagher Group Limited

4 Known issues

Controller Firmware Test

If you are running Command Centre vEL8.20 or later release, Controllers using vGR8.10 or earlier firmware version are not flagged by the Controller Firmware Test. In this case, manually check that your Controllers are using the firmware version that aligns with your Command Centre version.

Files Not Tampered Test fails after certain ClickOnce Client upgrade

Gallagher has found a rare instance where after upgrading any type of ClickOnce Client on a workstation, the file directory of the old version remains, causing the Files Not Tampered Test to fail. You should find the location of the old file directory in the Detected Installations section of the Security Health Check utility (by default, it is under AppData\Local\Apps\2.0\), and delete the old directory.

Utility takes too long to run

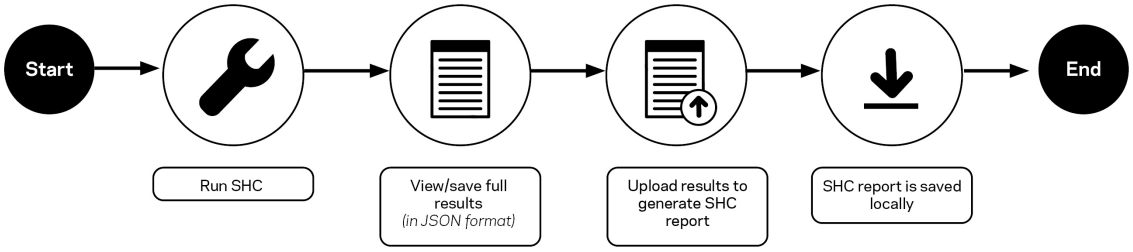
Gallagher has found that certain tests, particularly the Cross Controller Alarm Zones Test, can consume a large amount of time and server resources when running the Security Health Check. If the Cross Controller Alarm Zones Test is stopping the utility from running successfully, it can be skipped when running the utility via command line with the following command:

```
SecurityHealthCheck.exe -gui -skip 05280324-C57D-4B6F-8407-F45C9CCE10F3
```

Contact the Gallagher Support Team if you think you need to skip a different test or have a different issue (see last page of this document).

Copyright © Gallagher Group Limited

Appendix A: Security Health Check Process Map



Copyright © Gallagher Group Limited

Disclaimer

This document gives certain information about products and/or services provided by Gallagher Group Limited or its related companies (referred to as "Gallagher Group").

The information is indicative only and is subject to change without notice meaning it may be out of date at any given time. Although every commercially reasonable effort has been taken to ensure the quality and accuracy of the information, Gallagher Group makes no representation as to its accuracy or completeness and it should not be relied on as such. To the extent permitted by law, all express or implied, or other representations or warranties in relation to the information are expressly excluded.

Neither Gallagher Group nor any of its directors, employees or other representatives shall be responsible for any loss that you may incur, either directly or indirectly, arising from any use or decisions based on the information provided.

Except where stated otherwise, the information is subject to copyright owned by Gallagher Group and you may not sell it without permission. Gallagher Group is the owner of all trademarks reproduced in this information. All trademarks which are not the property of Gallagher Group, are acknowledged.

Copyright © Gallagher Group Ltd 2025. All rights reserved.

Copyright Notice

The software contains proprietary information of Gallagher Group Limited; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Gallagher Group Limited and the client and remains the exclusive property of Gallagher Group Limited. If you find any problems in the documentation, please report them to us in writing. Gallagher Group Limited does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Gallagher Group Limited.

Disclaimer

The terms “us” and “we” refer to Gallagher Security, a business unit of Gallagher Group Ltd. (GGL). The term “you” refers to the site representative or certified Channel Partner of a site running the Security Health Check (SHC) utility.

The SHC does not check for every possible security vulnerability nor constitutes a full penetration test of your system. It is designed to highlight areas of weakness so that you are better able to address them. The score is indicative only, and constitutes Gallagher's advice on any given test parameter at the time of testing.

We recognize that some sites may have valid reasons to configure settings that in most cases would not be. In this case, your SHC results may appear to be worse than expected. Please do not be concerned if this is the case for you; we intend to allow a means to bypass this consideration over time so that such intentional configurations do not affect your score.

Data Storage Terms

You may choose to submit data from your site in the form of a summarized file. The summarized file will identify you by a site ID number and will not contain site-specific information (such as item names, operator names or any personal information). We will use this data to generate and provide you with a ‘Security Health Check Report’ which will include your site name (as specified by you), but not its ID number.

You must comply with all applicable laws in connection with the use of the Security Health Check, including those relating to data privacy. Please refer to Gallagher's full privacy statement: https://www.gallagher.com/privacy-full

Any information that we provide to you relating to the Security Health Check is provided solely for your internal business purposes. You may not disclose or use any information provided to you relating to the Security Health Check for any other purpose or provide the information to any third party (other than to your Gallagher products supplier).

We will securely store the summarized file and any related information in an encrypted database. The information security of our database solution has been evaluated ("penetration tested") by third-party experts to ensure it meets our stringent requirements. Please contact Gallagher's technical support team for more information regarding third-party testing, or to see an executive summary of the results.

We may use the information you provide to conduct research and development, for technical support, for marketing purposes, and to optimise the performance of your site (including to obtain a better understanding of common security misconfigurations, to tailor future features to address these concerns, and to analyze security trends over time). We will only provide information relating to your Security Health Check results to you, your supplier of Gallagher products, our contractors or agents (on a need to know basis) or to other third parties if required by law.

Any data that you submit through the Security Health Check process will be stored and maintained in Gallagher's databases. This data can be removed at your request at any time by contacting Gallagher's technical support team at security.support@gallagher.com. Unless you request the removal of data, we will retain this data on our databases (which may be based in New Zealand or overseas).

We own all intellectual property rights in the Security Health Check tool and title in these intellectual property rights, and any modifications, improvements or other alterations, will at all times remain our property.

You acknowledge that we do not provide any representations or warranties of any kind in relation to the Security Health Check and, to the extent permitted to law, we disclaim all warranties, express or implied, relating to the Security Health Check. All information and other services we provide to you through the Security Health Check are on an “as is” basis and there is no warranty that the information or services will be error-free. Security Health Check does not constitute a full penetration test of your system. The provided score is indicative only and represents our recommendations at the time of testing. We will not be liable for any damages of any kind (including any direct, indirect, incidental and consequential damages) arising from the use of the Security Health Check or any information or other services provided to you from the Security Health Check.

Gallagher Group Limited is a global organization with headquarters based in New Zealand.

You can also find a copy of these terms and conditions at security.gallagher.com/shc

Copyright © Gallagher Group Limited

Contact Us

If you have any questions, complaints, comments or concerns about the Security Health Check, please contact Gallagher Technical Support, Customer Service, or the Security Health Check team.

Gallagher Tech Support Team:	+64 7 838 9894 | security.support@gallagher.com
Customer Service:	0800 84 2273
Feedback:	shc@gallagher.com

Copyright © Gallagher Group Limited