i

Release Notes

AHS-HF-5230-GU6052

Last Updated: 15 May 2020

The information contained in this document represents the current view of Accops Systems Private Limited on the issues discussed as of the date of publication. Because Accops Systems Private Limited must respond to changing market conditions, it should not be interpreted as a commitment on the part of Accops Systems Private Limited. Accops Systems Private Limited cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. ACCOPS SYSTEM PRIVATE LIMITED MAKES NO WARRANTIES, EXPRESSED OR IMPLIED IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the explicit written permission of Accops Systems Private Limited.

Contact Accops Systems Private Limited.
Email: info@accops.com
Call: +91 9595 277 001

CONTENTS

OVERVIEW

This document outlines the fixes provided in Hotfix AHS-HF-5230-GU6052 and how to apply hotfix on HySecure gateway. It is recommended to apply this hotfix on gateway version 5.2.3.0.

Note: Down time is required while applying this hot fix.

AHS-HF-5230-GU6052

Released on 15th May 2020

HOW TO APPLY HOTFIX

UPGRADE COMPATIBILITY OF HOTFIX AHS-HF-5230-GU6052

HySecure Hotfix AHS-HF-5230-GU6052 can be applied to **either of the below** mentioned HySecure gateway Setup:

- Accops HySecure gateway V5.2.3.0 with hotfixes applied in this order: **5232→5235→5236→6017→6026→6028→6033→6042→6048**
- Accops HySecure gateway V5.2.3.0 with hotfixes applied in this order: **5232→5235→5236→6017→6026→6028→6033→6034→6042→6048**
- Accops HySecure gateway V5.2.3.0 with hotfixes applied in this order: **6026→6028→6033→6042→6048**
- Accops HySecure gateway V5.2.3.0 with hotfixes applied in this order: **6026→6028→6033→6034→6042→6048**

Please refer section Appendix A: Upgrading HySecure cluster gateway for procedure to upgrade **HySecure cluster gateway**.

HOW TO GET HYSECURE HOTFIX AHS-HF-5230-GU6052

Download link for HySecure Hotfix AHS-HF-5230-GU6052:
https://propalmsnetwork-my.sharepoint.com/:u:/g/personal/support_accops_com/Ef57M3hFbhxDttr_bZsLG6oBzFAw04phKw-kCbWucoVYSQ?e=8krgPt

MD5 Checksum of HySecure Hotfix AHS-HF-5230-GU6052: **73283772262ccdb1829e825dc39adaf9**

NEW FEATURES IN HOTFIX AHS-HF-5230-GU6052

ADDED UNIQUE ID DEVICE PARAMETERS IN DEVICE ID ACCESS CONTROL

In this hotfix, we have added Unique ID device parameters in Device ID access control to identify USB based OS like Accops Nano OS.

Note: **Clearing browser cache is recommended.**

ISSUES FIXED IN HOTFIX AHS-HF-5230-GU6052

SECURITY OFFICER UNABLE TO ACCESS RDP APPLICATION FIX

In this Hotfix, we have fixed an issue where security officer user was unable to access RDP application

PROGENERIC CRASH AND FESIDLETIMEOUT CRASH

In this Hotfix, we have fixed an issue where Progeneric and fesidletimeout may get crash.

MEMORY LEAK IN FESDBSYNC

In this Hotfix, we have fixed memory leak issue in fesdbsync.

ENHANCE IDLETIMEOUT FEATURE

In this Hotfix, we have fixed Idle timeout issue in some cases. We have removed dependency of appcount for idle timeout.

OTP TOKEN NOT WORKING AFTER RESTORING USER BACKUP

In this hotfix, we have fixed an issue where users were unable to receive OTP token after restoring user backup from HySecure V5230 gateway.

ADDED SUPPORT TO RESTART FESNOTIFYPROXY & FESEMAILSUBSCRIBER USING MONITOR DAEMON

In this hotfix, we have enhanced Monitor daemon to start FesNotifyProxy & fesEmailSubscriber in case they crash.

ENHANCED HTTP RESPONSE HEADERS

This hotfix introduces support for Content-Type-Options HTTP response header sent as part of every response.

SENSITIVE DATA DISCLOSURE FIX

This hotfix fixes disclosure of internal IP addresses when accessing gateway resources using a specially crafted request.

KNOWN ISSUES IN HOTFIX AHS-HF-5230-GU6052

DEVICE ID POLICY RESTRICTION IF RELATED PARAMETERS ARE NOT SELECTED

If related parameters are not selected in device ID access control, then users may get message 'Login denied due to device restriction policy.' For e.g. if user is logging through browser and browser type & browser ID are not selected as device parameters then users may get above message while trying to login from approved browser.

HOTFIX UPGRADE LOG MAY NOT GENERATE ON STANDBY NODE

In some cases, hotfix upgrade log and admin log of applying hotfix may not generate on standby node.

Workaround: To confirm that Hotfix is applied please read below log file ***/tmp/.upgrade.log*** through SSH. Earlier mentioned file is hidden type, it will not be visible by ls command.

APPENDIX A: UPGRADING HYSECURE CLUSTER

The section describes the detailed process to apply hotfix on HySecure Cluster having three nodes (Active, Standby and Real Gateway server):

To upgrade HySecure cluster, follow these main steps:

- Upgrade the HySecure real Node
- Upgrade the HySecure standby Cluster Manger Node
- Upgrade the HySecure active Cluster Manger Node

UPGRADING REAL HYSECURE CLUSTER NODE:

- Connect to Real HySecure Cluster node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Real node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and enable maintenance mode.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

UPGRADING STANDBY HYSECURE CLUSTER MANAGER NODE:

- Connect to Standby HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and enable maintenance mode.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

UPGRADING ACTIVE HYSECURE CLUSTER MANAGER NODE:

- Connect to Active HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Active node**.**

- Login as security officer.
- Now go to "Upgrade Firmware" page under "Host Maintenance" Section => Select option ***Hotfix or service pack*** and upload the HySecure hotfix file.
- It may take 1 minutes or more to upload the hotfix based on network bandwidth between your PC and Gateway.
- Once the hotfix file is uploaded and upgrade is started, the message will be displayed on the browser. In some cases, the message may not come on the management console. Refresh the browser and see if the upgrade has completed.
- After hotfix is applied successfully.
- Go to "Upgrade Firmware" page under "Host Maintenance" Section and click on ***View Logs*** button to check the hotfix installation logs.

DISABLING MAINTENANCE MODE IN STANDBY NODE

- Connect to Standby HySecure Cluster Manager node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of Standby node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and disable maintenance mode.

DISABLING MAINTENANCE MODE IN REAL NODE

- Connect to Real HySecure node as Security Officer.

Note: Do not connect using Virtual IP Address, use the actual IP of real node**.**

- Login as security officer.
- Now go to "HA enable/disable" page under "High Availability" section and disable maintenance mode.

CLEAR BROWSER CACHE FOR HYSECURE MANAGEMENT CONSOLE PAGE

Clear browser cache so that new unique ID parameter become visible in HySecure Management console.

About Accops

Accops Systems Private Limited. under "Accops" brand is a globally leading developer and provider of Enterprise Mobility solutions involving Application and Desktop Virtualization, Secure Remote Access and Privilege Access Management solutions.

Accops' software and hardware products enable businesses to efficiently virtualize, secure and deliver business applications, corporate workspace and network services to their employees, partners, vendors, home users and mobile users, enabling instance access from anywhere using any device.

Tel: India +91 9595 277 001 | Europe +49 341 3315 78 30
Email: sales@accops.com | Web: www.accops.com